НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____201_ р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.170101 “Безпека інформаційних і комунікаційних систем”
(код і назва)

на тему: Атака на ланцюг постачання

Виконала: студентка 4 курсу, групи ФБ-51
(шифр групи)

Нікітюк Вікторія Анатоліївна _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник в.о. зав. каф., доцент Грайворонський М.В. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.170101 "Безпека інформаційних і комунікаційних систем"
(код і назва)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____201_ р.

ЗАВДАННЯ
на дипломну роботу студенту
Нікітюк Вікторії Анатоліївні
(прізвище, ім'я, по батькові)

1. Тема роботи Атака на ланцюг постачання,
науковий керівник роботи в.о. зав. каф., доцент Грайворонський М.В.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від « 27 » травня 2019 р. № 1414-С

2. Термін подання студентом роботи _____

3. Об'єкт дослідження це атака на ланцюг постачання
_____

4. Предмет дослідження політика безпеки, що має вразливі місця до досліджуваної атаки, та можливі методи захисту від неї
5. Перелік завдань, які потрібно розробити аналіз успішно реалізованих атак та аналіз можливих вразливих місць в ланцюгу постачання, визначення найефективніших методів захисту, вдосконалення існуючих методів захисту, створення власної формули для оцінки небезпеки загрози для компанії та побудова моделі захисту від атаки на ланцюг постачання для інформаційної системи компанії, оцінка ефективності створеної моделі.

6. Орієнтовний перелік ілюстративного матеріалу схема ланцюга поставок, споживча демографія CCleaner, знімок екрану системи, скомпрометованої Nyetya, тенденції атак в ланцюжку поставок програмного забезпечення, процес створення та функціонування абстрактної компанії, можливі вразливі місця в процесі розвитку і становлення компанії

7. Орієнтовний перелік публікацій «Атака на ланцюг постачання»

8. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1.	Вибір тематики роботи.	9.2018 – 10.2018	виконано
2.	Опрацювання необхідної літератури.	10.2018 – 11.2018	виконано
3.	Збір необхідних відомостей про атаки.	11.2018 – 12.2018	виконано
4.	Проведення необхідних досліджень.	1.2019 – 2.2019	виконано
5.	Складання структури побудови моделі захисту.	1.2019 – 2.2019	виконано
6.	Розробка моделі захисту.	2.2019 – 4.2019	виконано
7.	Перевірка ефективності створеної моделі.	4.2019 – 5.2019	виконано

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ _____
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника дипломної роботи.

РЕФЕРАТ

Представлена робота обсягом 69 сторінок містить 6 ілюстрацій, 6 таблиць та 23 джерела за переліком посилань.

Об’єктом дослідження є атака на ланцюг постачання.

Предметом дослідження є політика безпеки, що має вразливі місця до досліджуваної атаки, та можливі методи захисту від неї.

Методами дослідження було обрано: аналіз, моделювання, методи дедукції, імовірнісні (статистичні) методи.

Наукова новизна. В ході проведення дослідження було вперше створено формулу оцінки небезпеки та за її результатами – модель захисту від атаки.
Результати дослідження, які є основою дипломної роботи, були опубліковані в статті «Атака на ланцюг постачання». Стаття опублікована в збірнику, що містить матеріали XVII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики».

Ключові слова: ПОЛІТИКА БЕЗПЕКИ, АТАКА НА ЛАНЦЮГ ПОСТАЧАННЯ, ЗАГРОЗА, МЕТОДИ ЗАХИСТУ.

ABSTRACT

This work of 69 pages contains 6 illustrations, 6 tables and 23 literature references.

The object of the research is the supply chain attack.

The subject of the study is a security policy that has vulnerabilities to the attack being investigated and possible methods of protection against it.

The research methods were chosen: analysis, modeling, methods of deduction, probabilistic (statistical) methods.

Scientific novelty. In the course of the research, a formula for hazard assessment and its results - the model of protection against attack - was first created. The results of the research, which are the basis of the thesis, were published in the article "A supply chain attack". The article is published in the collection containing the materials of the XVII All-Ukrainian Scientific and Practical Conference of Students, Aspirants and Young Scientists "Theoretical and Applied Problems of Physics, Mathematics and Informatics".

Key words: SECURITY POLICY, SUPPLY CHAIN ATTACK, THREAT, PROTECTION METHODS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DDoS – Distributed Denial-of-service attack.

DoS – Denial-of-service attack.

USB – Universal Serial Bus.

ПК – персональний комп’ютер.

SSN – Social Security number.

FTP – File Transfer Protocol.

CVV – Card Verification Value.

VGA – Video Graphics Array.

SMB – Server Message Block.

API – Application Programming Interface.

DGA – Domain Generation Algorithms.

DNS – Domain Name System.

TSP – Time Stamp Protocol.

PDF – Portable Document Format.

Ip-адрес – Internet Protocol address.

PCI DSS – Payment Card Industry Data Security Standard.

IT-директор – Information Technology директор.

EDR – Endpoint Detection and Response.

MITM – Man In The Middle.

ВСТУП

Отримання несанкціонованого доступу до системи створює шлях для завантаження шкідливого ПЗ до створеного продукту і поширення інфікованої програми усім користувачам. Це ефективний спосіб за короткий проміжок часу вивести з ладу комп'ютери користувачів та за допомогою вимагання отримати багато грошей. Так як результат – великий обсяг даних користувачів, то зловмисники все частіше використовують цей метод збагатитись. І як виявилось на практиці, сучасні системи не в змозі створити ефективний захист від даної атаки, що стає все складнішою кожного дня.

Актуальність роботи зумовлюється тим, що на даний момент створена політика безпеки не ефективно захищає інформаційну систему підприємства від атаки на ланцюг постачання. У 2011 році було зафіксовано 1 атаку такого типу, а у 2017 вже 7. Так як за мінімальні проміжки часу можливо інфікувати більшу частину користувачів даного підприємства. Атака може початися на будь-якому етапі процесу розвитку і становлення та вражає всю інформаційну систему. Тому вирішення даної проблеми створить більш ефективну систему захисту.

Мета роботи – підвищення рівня захищеності інформації в інформаційній системі підприємства, шляхом виявлення і оцінки небезпеки загроз, створення та застосування ефективних рішень, які допоможуть зупинити атаку на початковому етапі.

Для досягнення даної мети були поставлені наступні **завдання**:

1) аналіз успішно реалізованих атак та аналіз можливих вразливих місць в ланцюгу постачання;
2) створення переліку загроз у кожному етапі ланцюга постачання, визначення найефективніших методів захисту, вдосконалення існуючих методів захисту, створення власної формули для оцінки небезпеки загрози для компанії та побудова моделі захисту від атаки на ланцюг постачання для інформаційної системи компанії;
3) оцінка ефективності створеної моделі.

Об’єктом дослідження є атака на ланцюг постачання.

Предметом дослідження є політика безпеки, що має вразливі місця до досліджуваної атаки, та можливі методи захисту від неї.

Методами дослідження було обрано: аналіз, моделювання, методи дедукції, імовірнісні (статистичні) методи. А точніше опрацювання літератури за даною темою, аналіз причин виникнення даної атаки, аналіз методів захисту, оцінювання небезпеки загрози і створення моделі захисту інформації від атаки на ланцюг постачання.

Наукова новизна. В ході проведення дослідження було вперше створено формулу оцінки небезпеки та за її результатами – модель захисту від атаки.

Практичне значення полягає в тому, що результати роботи можуть застосовуватись при створенні політики безпеки для компанії, що містить інформацію з обмеженим доступом.

Результати дослідження, які є основою дипломної роботи, були опубліковані в статті «Атака на ланцюг постачання». Стаття опублікована в збірнику, що містить матеріали XVII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики».

1 РОЗГЛЯД ПРИНЦИПУ ДІЇ ТА НАЙБІЛЬШІ ВИПАДКИ УСПІШНОЇ РЕАЛІЗАЦІЇ АТАКИ НА ЛАНЦЮГ ПОСТАЧАННЯ

Ланцюг постачання (supply chain): Взаємопов'язаний набір ресурсів і процесів, який починається з оформлення контракту на поставку, триває процесом отримання сировини, виробництвом, обробкою і закінчується передачею товарів та належних до них послуг кінцевому користувачеві. Ланцюг поставок може включати в себе продавців, промислові підприємства, логістичні центри, внутрішні центри розподілу, дистриб'юторів, оптових продавців та інших юридичних осіб, що беруть участь у виробництві, обробці та доставці товарів та належних до них послуг.[18]

Атака на ланцюг постачання – це кібератака, що здійснюється, використовуючи довіру між компанією-виробником та її клієнтами. Вона завдає шкоду організації, орієнтуючись на слабкі місця у ланцюгу постачання. Особливість цієї атаки у тому, що помічають втрату персональних даних або важливої інформації набагато пізніше, ніж проведено було атаку.

1.1 Схема дії атаки на ланцюг постачання

Зловмисник ставить під загрозу один або кілька компонентів процесу розробки чи доставки. Така атака може використовувати підроблені чіпи, що задіяні у виробництві комп'ютера або мережевого обладнання. Або, атака може запровадити скомпрометований код у програмному засобі, що не викликає підозри, як це було зроблено в атаках Nyetya і CCleaner. Є цілий ряд різних сценаріїв та методів, але головне, що ця атака використовує надійні канали для проникнення, щоб досягти своїх цілей.[1]

Отже, в який момент можна інфікувати комп’ютер злочинним кодом?! Ми можемо роздивитися схему ланцюга поставок (див. рис. 1.1). Потенційно кожна сторона має вразливе місце і на будь-якому етапі можна замінити чіп на

підроблений, встановити заражену програму, налаштувати обладнання так, щоб атаку можна було розпочати у будь-який момент.

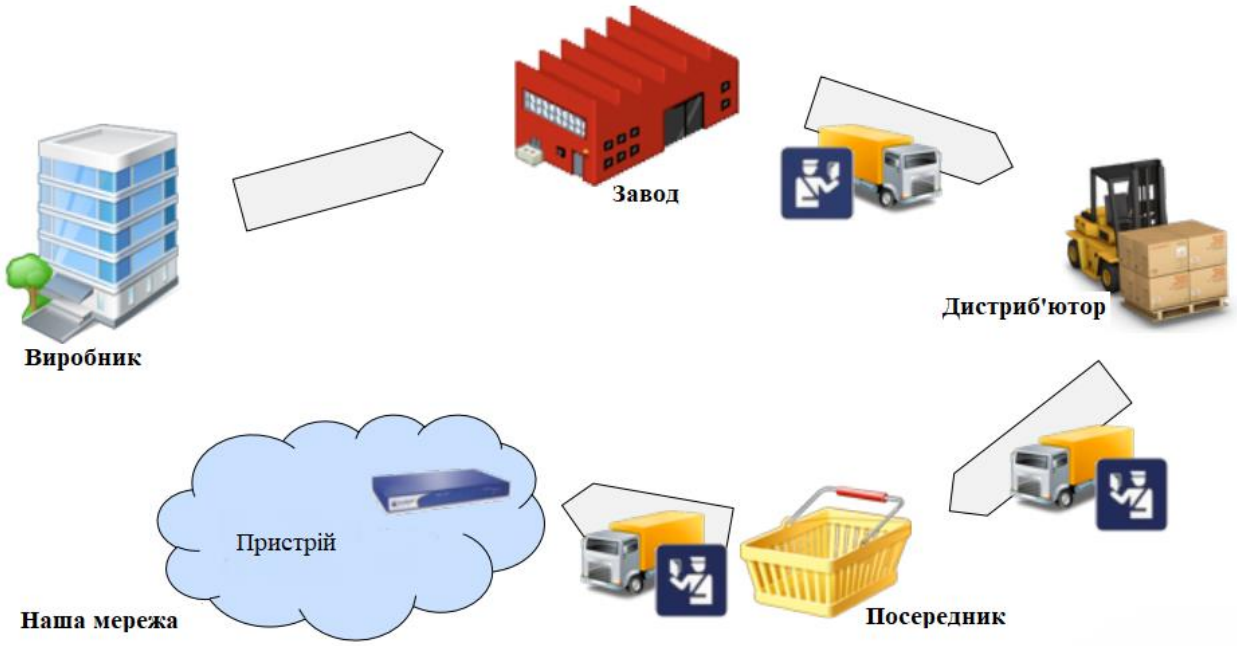

Рисунок 1.1 – Схема ланцюга поставок

Але перші атаки були проведені у 2013 році, кожна наступна була хитрішою та витонченою. Їх стратегії ставали складнішими і не зрозумілими. Якщо спочатку злочинці хотіли грошей, то з часом вони намагалися добратися до великих фірм.

1.2 Особливості реалізації атаки на ланцюг постачання

«Ланцюжок поставок» зазвичай має на увазі переміщення фізичних предметів, але в світі, де цифрові активи часто перевищують вартість фізичних активів, концепція ланцюжка поставок повинна бути розширена, щоб включати інформацію та послуги. Організації всіх типів покладаються на Інтернет і різні програмні інструменти та постачальників послуг для замовлення та оплати поставок, обміну інформацією з діловими партнерами і ведення бізнесу з клієнтами. Переривання цих процесів, навіть для компаній, що працюють в цегляному світі, потенційно може бути навіть більш руйнівним, ніж пошкодження транспортної інфраструктури. Такі компанії, як Advisen Ltd., чия

продукція в основному цифрова, можуть бути пошкоджені, якщо їхні постачальники інформації або постачальники цифрової інфраструктури не в змозі працювати.

Майже кожна компанія відчуває проблеми, пов'язані з несправністю програмного або апаратного забезпечення. Зазвичай ці події це трохи більше, ніж незручності, хоча іноді комп'ютерні проблеми можуть бути руйнівними. Австралійський компанія, яка поширювала свою продукцію через Amazon.com була заражена трьома рядками коду, призначеного для автоматичного генерування гасел з електронних словників та списків дієслів. Без відома компанії, поки не стало занадто пізно, Amazon рекламував футболки з повідомленнями, які протирічили політиці компанії.

Більш розповсюдженим сценарієм є неможливість функціонування через збій, пов'язаний з комп'ютером. В що спочатку було повідомлено про атаку hactivist колективу Anonymous, веб-хост GoDaddy був закритий протягом шести годин у вересні 2012 року через серію внутрішніх мережевих подій, які пошкодили таблиці даних маршрутизатора, хоча він є найбільшим у світі постачальником провайдерів захищених веб-сайтів з більш ніж 53 мільйонами зареєстрованих доменних імен.

Перерва торкнулася не тільки самого GoDaddy, але і багатьох компаній, які ведуть бізнес через веб-хостинг. Зростаюче занепокоєння для компаній - це зловмисні атаки на сайти та мережі. Ці напади можуть встановити зв'язок з кібер-злочинцями, які прагнуть отримати доступ до цінної інформації; хактивістів або терористичних груп, які прагнуть цього - шкоди компаніям, які вони вважають порушенням політичних, релігійних чи культурних переконань; або національні держави, що беруть участь у кібер-шпигунстві або навіть кібер-саботажі. Падіння жертви таких подій може зіпсувати репутацію компанії. Розглянемо наступні приклади:

- DigiNotar, голландська компанія, яка видала цифрові сертифікати, які проводили онлайн-транзакції, порушення безпеки призвели до видачі шахрайських сертифікатів.

- Великий американський метрополітен зазнав масової атаки «розподіленої відмови в обслуговуванні» (DDoS), яка вибила автоматизовані онлайн- та телефонні платіжні системи на 48 годин.
- Американська електростанція була знята з лінії протягом трьох тижнів, коли комп'ютерний вірус атакував турбінний контроль системи. Вірус був введений, коли технік, не знаючи, вставив інфікований комп'ютер USB в мережу.
- У тому, що вважається одним з найбільш руйнівних актів комп'ютерного саботажу на підприємстві на сьогоднішній день, а вірус видалив дані на три чверті корпоративних ПК нафтового гіганта – Saudi Aramco.

Кібер-атаки, як правило, орієнтовані на окремі організації або чітко визначену групу організацій, але вони мають потенціал для пошкодження бізнес-сектору або навіть цілої країни.[14]

1.3 Атака на Target — перша атака на ланцюг постачання

Перший випадок схожої атаки на атаку на ланцюг постачання був ще у далекому 2013 році. «70 мільйонів імен, адрес електронної пошти та телефонних номерів клієнтів американського роздрібного торговця Target (Target Corp. TGT: US) скомпрометовані в ході атаки на інфраструктуру компанії» — повідомляє сьогодні в своєму блозі Брайн Кребс. Реальний масштаб атаки розкритий самою компанією Target в офіційній заяві 10 січня.

Раніше Кребс говорив про меншу кількість записів, причому мова йшла не тільки про персональні дані, а й про платіжні реквізити - в ході хакерської атаки стався витік 40 мільйонів номерів кредитних карт. Потенційний збиток оцінити непросто. Мінімальна сума втрат, без урахування можливих позовів від клієнтів, складе сотні мільйонів доларів.

Доводиться з жалем констатувати, що аналітики InfoWatch мали рацію, попереджаючи про низький рівень захищеності платежів у «роздрібних

торговців». Витоку платежів складають майже половину (49%) від усіх витоків, що відбуваються в таких компаніях. При цьому в банках з платіжними даними пов'язано трохи менше третини всіх витоків - 29%. Трохи більша частка (31%) припадає на платіжні дані в процесингових компаніях. Основна причина - тотальне недотримання вимог PCI DSS – роздрібні торговці, всупереч усім заборонам зберігають інформацію про клієнтів, що не надійно захищена.

Постраждалим клієнтам Target пообіцяла безкоштовно відстежувати всі транзакції протягом року, щоб запобігти несанкціоноване списання грошових коштів. Цікаво, що така послуга зазвичай не потрібно в разі крадіжки даних про кредитні картки - їх власникам досить лише перевипустити саму карту. Очевидно, у Target є серйозні підстави припускати, що витекла не тільки платіжна інформація, але і значно більш «чутливі» дані, впевнений Кребс. У зв'язку з цим ситуація навколо витоку даних виглядає жахливо.

У базі Target, крім номерів кредитних карт і персональних даних, зберігалася номера соціального страхування (SSN) користувачів знижок програми Target. Ці дані широко використовуються при так званій «крадіжці особистості» (ID theft), коли зловмисники оформляють кредити на вкрадені номери страхування. Давно відомі схеми податкового шахрайства із застосуванням чужих SSN.

Пізніше Кребс повідомив про атаку на іншого торговця - Neiman Marcus - в ході якої також були вкрадені номери кредитних карт. Незважаючи на збіг термінів атаки (Neiman Marcus і Target атаковані в середині грудня), Брайан Кребс поки не готовий зв'язати ці події. The Wall Street Journal, посилаючись на анонімні джерела, повідомляє про 1 млн скомпрометованих записів. Крім Neiman Marcus і Target, є ще ряд компаній, які постраждали від атаки, повідомляє Bloomberg, цитуючи Уолтера Лоеба (Walter Loeb), президента консалтингової фірми Loeb Associates.[8]

Слідчі також поділилися додатковою інформацією про терміни злому і про те, як зловмисники забрали вкрадені дані з мережі Target. Джерела повідомили, що в період з 15 по 28 листопада (день подяки і день перед «чорною п'ятницею»)

зловмисникам вдалося завантажити шкідливе програмне забезпечення для крадіжки карт в невелику кількість касових апаратів в магазинах. Ті ж джерела повідомили, що зловмисники використовували цей час, щоб перевірити, що їх шкідливе ПЗ в точках продажів працює так, як було потрібно.

До кінця місяця, всього через два дні, зловмисники поширили свою шкідливу програму на більшість торгових точок Target і почали активно збирати записи з карт за транзакціями клієнтів в реальному часі, повідомили журналістам слідчі. Компанія Target заявила, що в період з 27 листопада по 15 грудня 2013 року в результаті злому було виявлено близько 40 мільйонів рахунків дебетових і кредитних карт.

Однак до січня 2014 року компанія підвищила цю оцінку, повідомивши, що особиста інформація 70 мільйонів її клієнтів була скомпрометована. Це включало повні імена, адреси, адреси електронної пошти та номери телефонів. Остаточна оцінка полягає в тому, що порушення торкнулося до 110 мільйонів клієнтів.

IT-директор Target подав у відставку в березні 2014 року, а його генеральний директор подав у відставку в травні. Нещодавно компанія оцінила вартість порушення в 162 мільйони доларів.

Дані викраденої картки були вивантажені за допомогою FTP-зв'язку в будь-яке місце в Росії, джерела, близькі до справи, кажуть, що значна частина вкраденої фінансової інформації була передана в кілька «віддалених» місць.

Це були в основному скомпрометовані комп'ютери в Сполучених Штатах і в інших місцях, які використовувалися для зберігання викрадених даних і до яких могли безпечно отримати доступ підозрювані злочинці в Східній Європі і Росії. Наприклад, дані карт, вкрадені з мережі Target, були збережені на зламаних комп'ютерних серверах, що належать бізнесу в Маямі, в той час як ще один віддалений сервер знаходився в Бразилії. Слідчі кажуть, що Сполучені Штати в даний час запитують взаємну правову допомогу у бразильських властей для отримання доступу до певних даних на сервері.[9]

1.4 Атаки на компанії British Airways та Ticketmaster

У вересні 2018 року одна з найвідоміших авіакомпаній British Airways, клієнтами якої є тисячі людей в усьому світі, виявила ситуацію, що стала катастрофою як для компанії, так і для усіх її користувачів: хтось скомпрометував більш ніж 380 000 транзакцій з банківськими картами клієнтів, які здійснювали платежі в авіакомпанію з 21 серпня до 5 вересня.

Зловмисники змогли отримати доступ не тільки до основної інформації про банківські картки користувачів (ПІБ і номер картки), але також і до кодів перевірки дійсності карток (CVV). Виникло питання, як вони змогли отримати ці коди, якщо навіть сама авіакомпанія їх не зберігає. Отже, був змінений скрипт на сайті авіакомпанії таким чином, щоб при здійсненні платежів хакери могли отримувати цей код разом з іншими даними. В результаті була здійснена крадіжка дуже великих масштабів та шкода репутації компанії.[2]

Клієнти компанії, у яких вкрали їх персональні дані, вже не зможуть довіряти цій платформі, отже компанія втратила багато грошей і відновити свою репутацію буде дуже складно. Так як зловмисники змогли отримати інформацію клієнтів, що має бути захищеною, то корпоративна інформаційна безпека вже серйозно порушена, і немає гарантій, що атака не повториться знову. Тим паче вже секретна інформація, яка важлива для компанії може бути в руках зловмисників, тобто політика безпеки порушена і діяльність компанії має бути зупинена на час, поки не буде встановлено всіх запобіжних заходів. Отже, атак створює серйозні наслідки, від яких страждають і користувачі, і співробітники, і сама компанія, і їх не можна виправити швидко і назавжди.

Звісно, постраждала від атаки на ланцюг постачання не тільки ця авіакомпанія. Є досить багато зареєстрованих випадків успішного проведення цієї атаки. Навіть за декілька місяців до цього інциденту, сайт з продажу квитків Ticketmaster повідомив про подібну крадіжку у якій постраждало 5%

користувачів сайту. Код одного із зовнішніх провайдерів був змінений так, щоб зловмисники могли отримати доступ до фінансовим даним клієнтів.

1.5 CCleaner - одна з ланок проведення атаки

Миколай Панков, один із працівників компанії Kaspersky Lab, зауважує: «Ми часто чуємо: «Ми маленька компанія, ми не цікаві організаторам APT!» Насправді це помилка. Ось, наприклад, історія з життя про те, як зловмисники використовували невелику організацію в ланцюжку атаки на великі компанії. На конференції з кібербезпеки Kaspersky Security Analyst Summit, колеги з AVAST розповіли про випадок з Piriform - невеликий британською компанією, яку AVAST купила в минулому році. Найвідоміший її продукт - застосунок CCleaner для чищення реєстру Windows. Випустили його давно, одним з перших серед аналогів, і число користувачів, що скачали його, вже перевалило за 2 млрд. Мабуть, тому зловмисники і вибрали саме цю програму для поширення шпигунського ПЗ.»

Як виявилось, то спочатку злочинці скомпрометували середу компіляції Piriform. Їм вдалося інфікувати сервер збірки застосунків, після чого програми з чистим вихідним кодом при компіляції отримували на додачу шкідливе ПЗ. Його потім і використовували для атаки. Причому за рахунок змін в бібліотеці компілятора інфіковане ПЗ отримувало справжній цифровий підпис Piriform. В результаті компанія розповсюджувала заражені CCleaner 5.33.6162 і CCleaner Cloud 1.7.0.3191.

Схема самої атаки була досить складною і складалася як мінімум з трьох етапів. Шкідливе ПЗ, запроваджене в популярну програму зі 100 млн активних користувачів, поширювалося цілий місяць. За цей час заражений CCleaner скачали 2,27 млн осіб, і як мінімум 1,65 млн екземплярів шкідливого ПЗ спробували зв'язатися з серверами зловмисників. Пізніше з'ясувалося, що на командному сервері працював простий скрипт, який вибирав жертв для другого

етапу атаки: ними ставали ті, хто, судячи по доменних іменах, міг виявитися співробітником великих IT-компаній та постачальників. На цьому етапі відібрали всього 40 комп'ютерів, на які потім відправили додаткове шпигунське ПЗ. На наступному етапі злочинці ще більше звузили список жертв: зібравши і проаналізувавши інформацію з цих 40 комп'ютерів (ймовірно, вже вручну), вони вибрали чотири найбільш цікаві цілі. На ці пристрої встановили спеціально доопрацьовану версію ShadowPad - відомого шкідливого ПЗ, яким вже користуються китайські кіберзлочинці. Це і було кінцевою метою атаки - доставити бекдор на комп'ютери певних співробітників великих компаній.[4]

Цей випадок досліджували фахівці з компанії Cisco Talos. 13 вересня 2017 року вони проводили бета-тестування своєї нової технології для виявлення експлоїтів і був знайдений файл, на який реагували їх системи захисту від шкідливих програм. Це був установник CCleaner v5.33 з легітимних серверів завантаження CCleaner. Talos провів первинний аналіз, щоб визначити, що змушує систему захисту блокувати CCleaner. Вони визначили, що, хоча завантажений виконуваний файл був підписаний з використанням дійсного цифрового підпису Piriform, CCleaner не був єдиною програмою, яку було завантажено. Під час установки CCleaner 5.33 32-розрядний двійковий файл CCleaner, також містив шкідливе навантаження з можливістю використовувати алгоритм генерації домену (DGA), а також функції видачі команд і управління (Command and Control - C2).

Також був виявлений другий зразок установника, пов'язаний з цією загрозою. Цей зразок також був підписаний з використанням дійсного цифрового сертифікату, проте відмітка часу підписання була приблизно на 15 хвилин пізніше підписання первісної збірки.

Наявність дійсної цифрового підпису у шкідливому двійковому коді CCleaner може вказувати на значну проблему, яка була причиною порушень в процесі розробки або підписання. В ідеалі цей сертифікат повинен бути відкликаний. При створенні нового сертифіката необхідно стежити за тим, щоб зловмисники не перебували в середовищі, в якому можна було б скомпрометувати новий

сертифікат. Тільки в процесі розслідування можливо було зібрати докладну інформацію про масштаби цієї проблеми і про те, як найкращим чином її вирішити.

З огляду на той факт, що двійковий код був підписаний цифровим підписом з використанням дійсного сертифіката, цілком ймовірно, що зловмисник із зовні скомпрометував частину середовища розробки або збірки і використовував цей доступ для вставки шкідливого коду в збірку CCleaner, яка була випущена організацією. Також можливо, що інсайдер, який має доступ до середи розробки або збірки всередині організації, навмисно включав шкідливий код або мав скомпрометований обліковий запис, який дозволяв зловмисникові змінювати код. Важливо відзначити, що, хоча попередні версії установника CCleaner в даний час доступні на сервері завантаження, версія, яка містить шкідливі файли, була видалена і більше не доступна.[5]

Спочатку записується поточний системний час в зараженій системі. Потім він затримується на 601 секунду перед продовженням операцій, що, ймовірно, є спробою обійти автоматизовані системи аналізу, які налаштовані на виконання вибірок протягом заздалегідь визначеного періоду часу або визначити, чи виконується шкідливе ПЗ в відлагоджувачі (debugger). Щоб реалізувати цю функцію затримки, шкідлива програма викликає функцію, яка намагається пропінгувати з використанням тайм-ауту, встановленого на 601 секунду. Потім він перевіряє поточний системний час, щоб дізнатися, чи пройшло 600 секунд. Якщо ця умова не виконується, шкідлива програма припиняє виконання, а бінарний файл CCleaner продовжує нормальну роботу. У ситуаціях, коли шкідлива програма не може виконати IcmpCreateFile, вона потім повертається до використання Sleep () для реалізації тієї ж функціональності затримки. Шкідлива програма також порівнює поточний системний час зі значенням, що зберігається в наступному розділі реєстру.

Потім зловмисна програма перевіряє, щоб визначити привілеї, призначені користувачеві, який працює в системі. Якщо поточний користувач, який виконує

шкідливий процес, не є адміністратором, шкідлива програма припинить виконання.

Якщо користувач, що запускає зловмисну програму, має адміністративні привілеї в зараженій системі, для цього процесу включається SeDebugPrivilege. Потім шкідлива програма зчитує значення «InstallID», яке зберігається в спеціальному розділі реєстру.

Після виконання вищезазначених дій шкідливе ПЗ починає профілювання системи і збір системної інформації, яка потім передається на сервер C2.

Як тільки системна інформація була зібрана, вона шифрується і потім кодується з використанням модифікованого Base64. Потім шкідлива програма встановлює канал командування і управління (C2).

При аналізі цієї шкідливої програми Talos виявив, що в шкідливий код, пов'язаному з функцією C2, присутня програмна помилка.

Як тільки сервер C2 був ідентифікований для використання шкідливою програмою, він потім відправляє закодовані дані, що містять інформацію про профілі системи, і зберігає IP-адреса C2 в певному місці реєстру. Потім шкідлива програма зберігає значення поточного системного часу плюс два дні.

У ситуаціях, коли первинний сервер C2 не повертає відповідь на запит HTTP POST, шкідлива програма повертається до використання алгоритму DGA. Алгоритм, який використовується цією шкідливою програмою, заснований на часу і може бути розрахований з використанням значень року і місяця.

Шкідлива програма ініціює пошук DNS для кожного домена, створеного алгоритмом DGA. Якщо пошук DNS не приводить до повернення IP-адреси, цей процес буде продовжений. Шкідлива програма виконає DNS-запит активного домену DGA і очікує, що дві IP-адреси будуть повернуті з сервера імен, керуючого простором імен домену DGA. Потім шкідлива програма обчислює вторинний сервер C2, виконуючи серію бітових операцій з повернутими значеннями IP-адрес, і об'єднує їх для визначення фактичної запасної адреси сервера C2, який буде використовуватися для наступних операцій C2.

В ході аналізу Cisco Talos зауважив, що домени DGA не були зареєстровані.

Вплив цієї атаки може бути серйозним, враховуючи надзвичайно велику кількість систем, які можуть бути зачіплені (див. рис. 1.2). CCleaner стверджує, що за станом на листопад 2016 року в світі було завантажено понад 2 мільярди завантажень, і, за повідомленнями, вона додає нових користувачів зі швидкістю 5 мільйонів в тиждень.

Рисунок 1.2 – Споживча демографія CCleaner[5]

Якщо навіть невелика частина цих систем буде зламана, зловмисник може використовувати їх для будь-якої кількості цілей. Уразливі системи повинні бути відновлені до 15 серпня 2017 року або перезавантажені. Користувачі також повинні оновитися до останньої доступної версії CCleaner, щоб уникнути зараження.

При аналізі даних телеметрії на основі DNS, пов'язаних з цією атакою, є значна кількість систем, які відправляють запити DNS, намагаючись дозволити домени, пов'язані з вищезгаданими доменами DGA. Оскільки ці домени ніколи не були зареєстровані, розумно зробити висновок, що єдині умови, при яких системи будуть намагатися дозволити пов'язані з ними IP-адреси, - це якщо на них впливало це шкідливе ПЗ. У той час як у більшості доменів, пов'язаних з цим DGA, майже немає трафіку запитів, пов'язаних з ними, домени, пов'язані з серпня

і вересня (що корелює з тим, коли ця загроза була активна), показують значно більшу активність. [5]

Це яскравий приклад того, наскільки зловмисники готові пройти через спробу поширення зловмисних програм серед організацій та окремих осіб по всьому світу. Використовуючи довірчі відносини між постачальниками програмного забезпечення і користувачами їх програмного забезпечення, зловмисники можуть отримати вигоду з властивою для користувачів довірою до файлів і веб-серверів, що використовуються для розповсюдження оновлень.

У багатьох організаціях дані, отримані від постачальників програмного забезпечення, не часто отримують такий же рівень перевірки, як той, який застосовується до того, що сприймається як ненадійні джерела. Зловмисники показали, що вони готові використовувати цю довіру для поширення шкідливого ПЗ, залишаючись при цьому непоміченими.

1.6 Найбільша атака в Україні — Petya.A

Атака на CCleaner тривала досить довго, і ніхто спочатку не помітив її. Але схожа атака була проведена раніше і була надто «гучною». 27 червня українські банки, енергетичні компанії, державні інтернет-ресурси і локальні мережі, українські медіа та інші великі підприємства зазнали найбільшої хакерської атаки, яка поширювала вірус Petya.A. (Diskoder.C), що блокує роботу комп'ютерних систем.

Компанія ISSP Labs провела моніторинг вірусної активності сайту Crystal Finance Millennium і виявили вірусну розсилку, в якій було знайдено зразок вірусу. «Скрипт є завантажувачем, основне завдання якого скачати і запустити виконуваний файл. Також критичні дані, такі як адреса, з якої буде завантажено шкідливий файл, який знаходиться в скрипті у вигляді тексту в масиві. Примітною особливістю зразка є адреса, з якої завантажується шкідливий файл

- cfm.com.ua. Згідно з публічною інформацією, цей сайт програмного комплексу бухгалтерського обліку Crystal Finance Millennium», - пояснили в компанії.

29 червня корпорація Microsoft знайшла докази поширення вірусу Petya.A. через програму бухгалтерського обліку M.E.Doc. 4 липня українська поліція конфіскувала сервери компанії з розробки бухгалтерського програмного забезпечення M.E.Doc за підозрою в поширенні вірусу Petya.A.[6]

В компанії Cisco Talos прийшли до висновку, вірус Petya.A небезпечний та лише був схожий на вимагач, втім його метою було знищення файлів. Він шифрує головний завантажувальний запис комп'ютера (можна сказати, «зміст» жорсткого диска). Потрапивши в систему, вірус автоматично поширюється трьома способами, один з яких - відома уразливість Eternal Blue, яку, до речі, використовував і вірус WannaCry. Спеціалісти компанії вирішили дослідити цю загрозу і отримали неочікуванні результати.

Після атак SamSam, які були спрямовані на медичні установи США в березні 2016 року, Cisco Talos був стурбований поширенням шкідливих програм через уразливості в мережі. В травнем 2017 року вимагач WannaCry скористався уразливістю в SMBv1 і поширився з великою швидкістю по Інтернету, знищуючи усе навкруги.

Сьогодні з'явився новий варіант шкідливого ПЗ, який настільки відрізняється від Petya.A, що люди називають його різними іменами, такими як Petrwrap і GoldenEye. Cisco Talos ідентифікує цей новий варіант шкідливого ПЗ як Nyetya. Зразок використовує EternalBlue, EternalRomance, WMI і PsExec для бокового переміщення всередині вразливою мережі. На відміну від WannaCry, Nyetya не містить зовнішній компонент сканування.

Ідентифікація вихідного вектора все ще розслідується. Фахівці з Cisco Talos не бачили дані про використання електронної пошти або документів Office в якості механізму доставки цієї шкідливої програми. Але вони вважають, що зараження пов'язане з системами оновлення програмного забезпечення для українського пакета податкової звітності під назвою MeDoc. Cisco Talos розслідує це нині.

З огляду на обставини цього нападу, Cisco Talos з великою впевненістю оцінює, що намір зловмисника, що стоїть за Nyetya, носило руйнівний характер і не було економічно вмотивованим. Cisco Talos настійно рекомендує користувачам і організаціям відмовитися платити викуп. Будь-які спроби отримати ключ дешифрування будуть безрезультатними, так як пов'язані поштову скриньку, що використовується для перевірки оплати і спільного використання ключа дешифрування, була закрита posteo.de. Це робить будь-який успішний платіж марним, оскільки для цього суб'єкта не існує способу зв'язку, який можна було б використовувати для перевірки платежів від жертв або поширення ключів дешифрування після отримання викупу. Шкідливі програми також не використовують метод прямого підключення до команд і контролю для віддаленого розблокування.[7]

Але цікаво як діяла атака. Perfc.dat містить функціональні можливості, необхідні для подальшої компрометації системи, і містить одну безіменну функцію експорту, звану # 1. В рамках процесу поширення шкідлива програма перераховує всі видимі машини в мережі через виклик API NetServerEnum, а потім сканує відкритий порт TCP 139. Це робиться для складання списку пристроїв, які надають цей порт і можуть бути схильні до ризику.

Nyetya має кілька механізмів, які використовуються для поширення після зараження пристрою:

- EternalBlue - той же експлойт, який використовує WannaCry.
- EternalRomance - експлойт SMBv1, пропущений "ShadowBrokers"
- PsExec - законний інструмент адміністрування Windows.
- WMI - інструментарій управління Windows, законний компонент Windows.

Ці механізми використовуються для спроби установки і виконання perfc.dat на інших пристроях для поширення.

Для систем, які не мали MS17-010 застосовуються, експлойти EternalBlue і EternalRomance позикових коштів для злому систем. Експлойт, запущений проти системи жертви, залежить від операційної системи передбачуваної мети.

- EternalBlue
    - Windows Server 2008 R2
    - Windows Server 2008
    - Windows 7
- EternalRomance
    - Windows XP
    - Windows Server 2003
    - Windows Vista

Два експлойта відкидають модифіковану версію DoublePulsar, яка є постійним бекдором, які працюють в просторі ядра скомпрометованої системи. Розробник змінив тільки кілька байт в порівнянні з оригінальною версією, але ця зміна дозволила йому уникнути виявлення в мережі та інструментів сканування DoublePulsar з відкритим вихідним кодом, доступних в Інтернеті. Атакуючий змінив коди команд у таблиці 1.1 і відповідей у таблиці 1.2.

Таблиця 1.1 – Змінені коди команд.

Original Command Code	Nyetya Command Code	Purpose
0x23	0xF0	PING
0x77	0xF1	KILL
0xC8	0xF2	EXEC

Таблиця 1.2 – Змінені коди відповідей.

Original Response Code	Nyetya Response Code	Purpose
0x10	0x11	OK
0x20	0x21	CMD_INVALID
0x30	0x31	ALLOCATION_FAILURE

Зловмисник змінив положення, в якому код відповіді зберігається в пакеті відповіді SMB. У початковій версії DouplePulsar код був збережений в поле MultiplexID (зміщення 0x1E). У версії Nyetya код відповіді зберігається в зарезервованому поле (зміщення 0x16), яке зазвичай встановлюється в 0x0000 Реалізоване спеціальне правило NGIPS / Snort для виявлення цього варіанту DoublePulsar: 43459.

PsExec використовується для виконання наступної інструкції (де wxyz - IP-адреса) з використанням токена Windows поточного користувача встановити шкідливе ПЗ на мережевий пристрій.

WMI використовується для виконання наступної команди, яка виконує ту ж функцію, що і вище, але використовує ім'я користувача і пароль поточного користувача (як ім'я користувача і пароль).

Після успішного злому системи шкідлива програма шифрує файли на хості з використанням 2048-бітного RSA-шифрування. Крім того, шкідлива програма очищає журнали подій на скомпрометувати пристрої.

Nytetya намагається отримати адміністративні привілеї (SeShutdowPrivilege і SeDebugPrivilege) для поточного користувача через Windows API AdjustTokenPrivileges. У разі успіху Nyetya перезаписує завантажувальний сектор на PhysicalDrive0 без попереднього збереження копії. Якщо перезапис завантажувального сектора не вдався, Nyetya замість цього стирає перші десять секторів диска. Крім того, якщо Nyetya виявить в системі хеш імені файлу процесу 2E214B44, вона також зітре перші десять секторів диска. Cisco Talos визначив, що цей хеш посилається на avp.exe, який відповідає Антивірусу Касперського. Системи з перезаписати завантажувальний сектором побачать це повідомлення при перезапуску своїх систем.

Знімок екрану системи, скомпрометованої Nyetya (див. рис. 1.3).

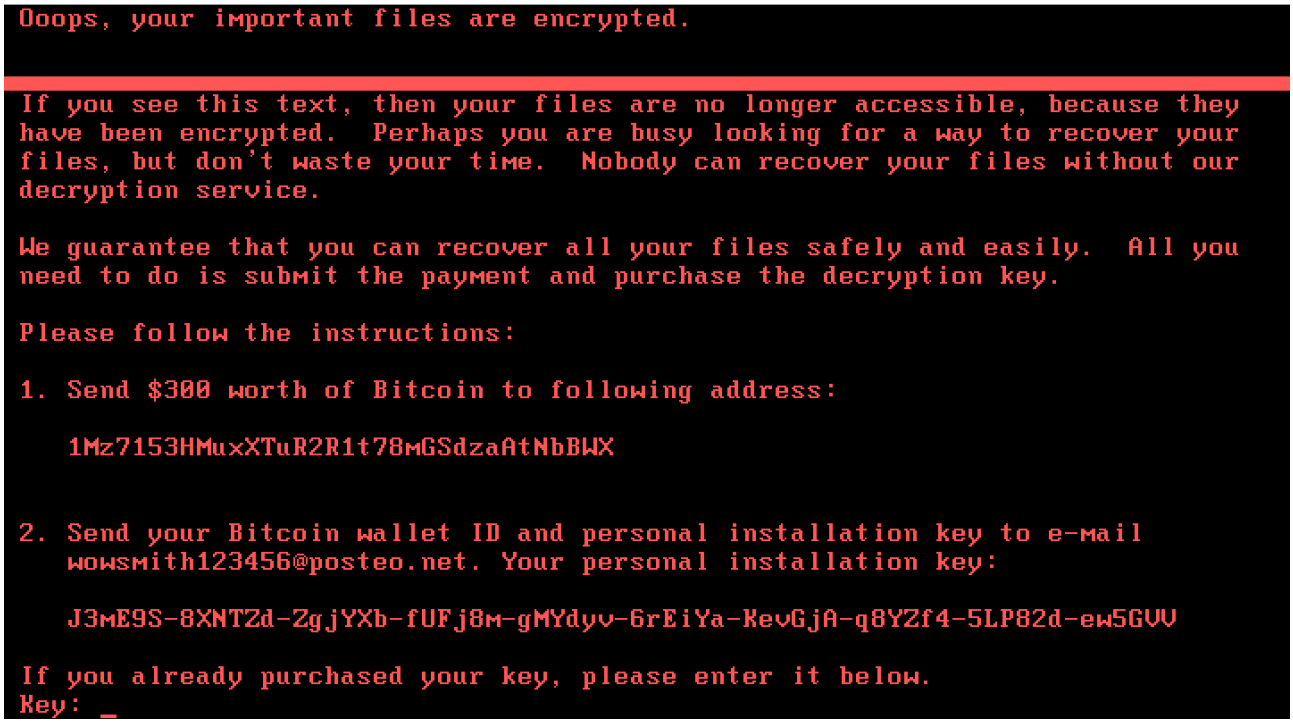

Рисунок 1.3 – Знімок екрану системи, скомпрометованої Nyetya

Незалежно від того, чи вдасться Nyetya перезаписати завантажувальний сектор чи ні, він продовжить створення запланованої завдання за допомогою schtasks для перезавантаження системи через годину після зараження.

Cisco Talos вважає, що, не аналізуючи генерацію ключів або компоненти зберігання ключів, дійові особи Nyetya не призначалися для завантажувального сектора або десяти секторів, які повинні бути відновлені. Таким чином, Nyetya повинен бути руйнівним, а не інструментом фінансової вигоди.[7]

Якщо проаналізувати усі атаки, то можна помітити, що їх мотиви можна поділити на дві категорії: політичні та економічні. І дуже дивно те, що атаки мали різні характери та наслідки. Якщо Nyetya була надто гучною атакою, про неї говорили усі ЗМІ та люди, які далекі від IT, знали про неї, то про CCleaner, довго навіть не здогадувались. І досягли вони різних цілей. З кожним роком атака стає більш небезпечною, адже спочатку метою було викрасти персональні дані та знищення інформації, то тепер атака дозволяє вирахувати спеціалістів великих компаній та завдати шкоди в набагато більших масштабах. Отже, як же атака може впливати на усю країну?!

Вірус зазвичай розповсюджується із шаленою швидкістю, і як розповів технічний директор української антивірусної компанії "Zillya" Олег Сич, швидке зараження відбувається через те, що комп'ютери працюють в локальній мережі. "Судячи з усього, це нова модифікація WannaCry, ми фіксуємо дуже багато спільного, навіть імена виконуваних файлів троянської програми залишилися аналогічними, а іноді – одні й ті ж. Тобто, належать тим же авторам".

Помітно, що Nyetya використовує протокол зв'язку в локальних мережах, тому зараження відбувається досить швидко саме всередині компаній. Звичайні користувачі, як правило, не використовують такий протокол зв'язку, тому піддаються зараженню значно рідше. А от в локальній мережі, де працюють сотні або тисячі користувачів, як організації, що вже заразилися, частіше за все об'єднані в одну локальну мережу, тому є набагато більш уразливими і заражаються моментально.

Всім організаціям, які постраждали від атаки, може загрожувати непоправна втрата інформації, яка зберігалася на їхніх комп'ютерах. Найгірше, якщо заразилися сервери компанії, а не просто робочі станції. "У нас є вже повідомлення від деяких клієнтів, у яких постраждали саме сервери - внутрішні і зовнішні. Тут все складніше, тому що на серверах якраз зберігаються всі копії даних. Втрата даних на серверах - найбільш критична. Зараз ставка тільки на резервні копії. У разі, якщо вони відсутні, на розшифровування вірусу піде не менше двох тижнів", - сказав Олег Сич.

Водночас він заспокоїв, що у банків, які потрапили під зараження, рівень загрози найменший, оскільки майже всі вони роблять резервне копіювання даних. "Все, що вони можуть втратити - кілька десятків хвилин або годин, вся інша інформація у них копіюється. Проблеми найчастіше виникають у організацій, які не роблять резервні копії", - додав Сич.[10]

Про це повідомив народний депутат та радник глави МВС Антон Геращенко у Facebook. За його словами, атака готувалася щонайменше місяць. Листи з вірусом, які надходили адресатам, були російською та українською

мовою. Зазначається, що у програмному коді вірусу була закладена дата запуску 27 червня об 11.00.

"Кібератака що має своєю кінцевою метою спробу дестабілізації ситуації в економіці і суспільній свідомості України, була замаскована під спробу вимагання грошей у власників комп'ютерів. Вірус зашифровує всі дані жорсткого диска і вимагає викуп у кілька сотень доларів. Метою цієї тренувальної кібератаки, швидше за все приуроченої до Дня Конституції України, є офіси банків, редакції засобів масової інформації, об'єкти зв'язку, транспорту, телекомунікації, енергетики", - каже Геращенко.

Вірус атакував "Укртелеком", "Київ" і "Дніпроенерго", "Укрзалізниця", аеропорт "Бориспіль", Кабінет Міністрів.[11]

Висновки до розділу 1

У першому розділі було розглянуто механізм роботи атаки на ланцюг постачання, її реалізацію та причини, чому актуальність даної проблеми збільшується. Наслідки успішної реалізації наносять шкоду будь-якій галузі промисловості. І будь-яка компанія може стати лише однією з ланок даної атаки. Дарма, що більшість власників середнього бізнесу вважають, що вони не можуть стати жертвою атаки на ланцюжок постачання. Адже вони перші кого атакують і використовують, щоб дібратися до більших компаній.

В даному розділі розглянуто найбільші атаки та проведено їх аналіз з метою виявлення особливостей атаки на ланцюг постачання. Атака на ланцюг поставок має складну структуру дії, її складно виявити і з’явитися вона може в будь-якому сегменті. Проаналізувавши, було виявлено вразливі місця, які потребують особливого розгляду. Також важливо відмітити, що атака проходить в декілька етапів та створюється стратегія для успішної реалізації атаки.

З цього випливає, що реалізувати атаку дуже складно і не під силу будь-кому. По-перше, для того, щоб знайти вразливе місце та проникнути в середовище розробки програмного забезпечення, що є ціллю для зловмисника,

потрібно багато часу та ресурсів. По-друге, сил та знань досвідчених програмістів, щоб створити атаку, що правдоподібно імітує усі процеси та непомітно впровадити злочинний код. Це має бути створена команда з фахівців, що знають яким чином захищена структура, яка є ціллю для нападу, зможуть написати заражений програмний код та впровадити його в певний комп'ютер, що є стратегічно важливим. Також це потребує не малих коштів.

Але якщо атаку вдасться здійснити, то зловмисники зможуть отримати персональні дані клієнтів, вивести з ладу техніку, знищити інформацію та викрасти велику суму грошей.

2 СТВОРЕННЯ МОДЕЛІ ЗАХИСТУ ВІД АТАКИ НА ЛАНЦЮГ ПОСТАЧАННЯ

На початку 2017 року виявлено операцію WilySupply, атаку, яка скомпрометувала засіб оновлення програмного забезпечення текстового редактора для завантаження бекдору на цільові організації в фінансовому та IT-секторах. Кілька тижнів потому чергова атака ланцюжка поставок потрапила в заголовки газет, ініціювавши глобальний спалах вимагачів. Підтверджено припущення про те, що процес оновлення програмного забезпечення для податкового обліку, популярного в Україні, був першим джерелом зараження для вимагачів Petya. Пізніше, в тому ж році, з скомпрометованої інфраструктури була доставлена версія популярного безкоштовного інструменту CCleaner з резервною копією. Потім, на початку 2018 року, виявлено і зупинено спалах Dofoil.

Це лише деякі з багатьох подібних випадків атак на ланцюжок поставок, які спостерігалися в 2017 і 2018 роках. З кожним роком кількість атак збільшується (див. рис. 2.1).

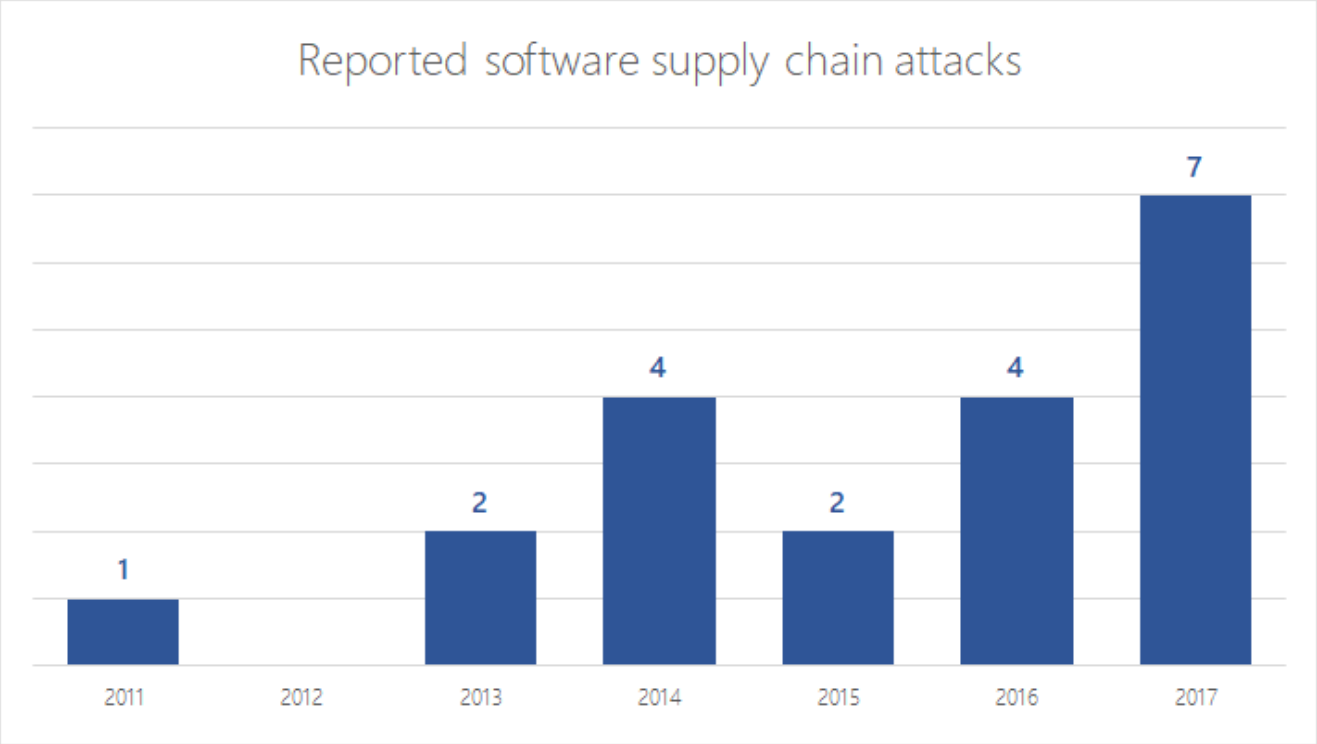

Рисунок 2.1 – Тенденції атак в ланцюжку поставок програмного забезпечення (джерело: презентація RSA Conference 2018 «Вектор несподіваних атак: засобу оновлення програмного забезпечення») [18]

Зростаюча поширеність атак по ланцюжку поставок може бути частково приписана посиленим сучасним платформам, таким як Windows 10, і зникнення традиційних векторів зараження, таких як експлойти браузера. Зловмисники постійно шукають найслабшу ланку; оскільки експлойти нульового дня стають занадто дорогими для покупки або створення (набори експлойтів знаходяться на історично нижчій точці), зловмисники шукають дешевші альтернативні точки входу, такі як компроміс між ланцюгами поставок програмного забезпечення. Вони використовують переваги небезпечних методів кодування, незахищених протоколів або незахищеної серверної інфраструктури постачальників програмного забезпечення, щоб полегшити ці атаки.

Вигода для зловмисників очевидна: ланцюжки поставок можуть запропонувати більшу базу потенційних жертв і можуть привести до великого прибутку. Спостерігалося, що воно призначене для широкого спектру програмного забезпечення і впливає на організації в різних секторах. Це

загальногалузева проблема, яка потребує уваги з боку багатьох зацікавлених сторін – розробників програмного забезпечення і постачальників, які пишуть код, системних адміністраторів, які управляють установками програмного забезпечення, і спільноти інформаційної безпеки, які виявляють ці атаки і створюють рішення для захисту від них, серед інших.

2.1 Схема захисту від атаки на ланцюг постачання

Атака на ланцюг поставок виявляється успішною, бо є багато вразливих фрагментів у системі захисту підприємства і не враховують дрібні деталі, що можуть в майбутньому бути першим елементом даної атаки.

Атака такого типу має свої особливості:

1. Компанії, які постраждали від атаки на ланцюг поставок, помічають втрату персональних даних та особливо важливої інформації набагато пізніше, ніж відбувся початок атаки, таким чином чим більше часу не припиняється атака, тим більше даних клієнтів скомпрометовано.
2. Використовується довіра користувачів до продукту, який вони вже спробували, і бездоганної репутації компанії, що піклуючись про клієнтів випускає оновлення свого продукту.
3. Зараження може відбутися ще в ланцюгу постачання компанії-постачальника, а інфікований продукт з’явиться вже в першій ланці ланцюга постачання компанії, що користується її послугами.
4. Її можна порівняти з бомбою уповільненої дії, тобто на певному етапі ланцюга постачання впроваджується заражений компонент (виконуваний файл, спеціальний програмний засіб і т.п.), який пізніше, при завантажені користувачами програми, починає діяти за сценарієм зловмисників, і за короткий проміжок часу може відкрити доступ або вивести з ладу мільйони комп’ютерів користувачів.

5. Початок процесу дії атаки може відбутися в будь-якій ланці створення і розвитку компанії. Для ефективної роботи використовуються дані розвідки, які були отриманні в результаті шпигунства за співробітниками, стратегічно важливими приміщеннями, технікою та способом життя підприємства.

Для створення моделі захисту розглянемо абстрактну компанію, яка має усі ланки, які б зловмисники використовували для створення дієвої атаки на ланцюг поставок. Не бачу сенсу розглядати компанію, яка не співпрацює з іншими та створює все обладнання, необхідні утиліти та програми, не користуючись послугами професіоналів, помічників і т.д.. Це утопія, яка коштує величезних грошей і не гарантує абсолютного захисту від цієї атаки.

Отже, розглянемо рис. 2.2, на схемі зображено процес створення та розвитку компанії, в аспекті появи вразливих місць, пов’язаних з використанням послуг постачальників з різних сфер. Перший етап схеми – це приміщення з не технічним обладнанням. Приміщення має бути створено або вибрано та облаштовано таким чином, щоб зводились до мінімуму можливості витоку інформації технічними каналами.

Рисунок 2.2 – Процес створення та функціонування абстрактної компанії

Для того, щоб компанія змогла облаштувати офіс спеціальною технікою їй необхідно звернутися до постачальника технічного обладнання та апаратних компонентів. Якщо у стратегію компанії входить створювати свої високотехнологічні компоненти, телекомунікаційне обладнання і тому подібне, то послуги надійного постачальника будуть необхідні, адже від нього в майбутньому буде залежати якість продукції, що виробляє дана компанія. Отже, це теж важлива ланка, якою неможливо знехтувати.

Ми маємо технічно забезпечений офіс, в якому вже можна працювати. Але не функціональний повністю, адже не має програмного забезпечення, яке вимагається для безпечної роботи, зв'язку усіх співробітників та середовище, в якому вони можуть працювати. Тоді керівництво вирішує який набір програм потрібен для кожного відділу та для усієї компанії в цілому.

Наступний постачальник – фірми з пошуку персоналу. Цей пункт можна уникнути, адже в компанії створюється відділ з такими функціями, але зазирнемо в майбутнє, і є два можливих варіанта розвитку подій. Перший скористуватися послугами фірми, що спеціалізується в даному питанні, має свій штат юристів, співробітників, які збирають досьє на кожну кандидатуру на відкриту вакансію, аналізують зібрану інформацію і визначають рівень та ризики для компанії пов'язані з кандидатом як майбутнім співробітником. Другий – створення відділу, який буде функціонувати як компанія з першого випадку, але це дуже не простий процес навчання і створення плану та положень дій для співробітників і наявність спеціаліста, який надав би досвід і знання, взяв би на себе відповідальність керувати даним відділом, але можливий і дорогий. На початку свого шляху компанії обмежені фінансово, то найлегшим варіантом було б спочатку використовувати перший варіант, а згодом створити свій відділ. Схожий сценарій мають і фірми, які надають послуги з забезпечення інформаційної безпеки. Але в цьому випадку краще створити власний відділ, тому що програмний продукт, який випускають, має бути безпечним, і формування політики безпеки для кожної компанії має свої тонкощі.

В результаті, компанія випускає утиліти, які доступні для завантаження з веб-сайту і в подальшому з можливістю завантаження оновлень, та програмне та апаратне забезпечення, яке можна придбати або через онлайн сервіс, або спеціальному магазині.

Тепер детальніше обстежимо вразливі місця і на якому етапі вони з’являються. Розглянемо рис. 2.3, на схемі з’явилися стрілки різних кольорів. Це можливі варіанти атаки. Класифікацію здійснено в залежності від типу постачальника та об’єкта атаки. Проведемо аналіз атаки на ланцюг поставок на кожному етапі методом виявлення можливих загроз, втрат та знаходження рішень для нейтралізації цих загроз або зведення до мінімуму можливості їх успішної реалізації.

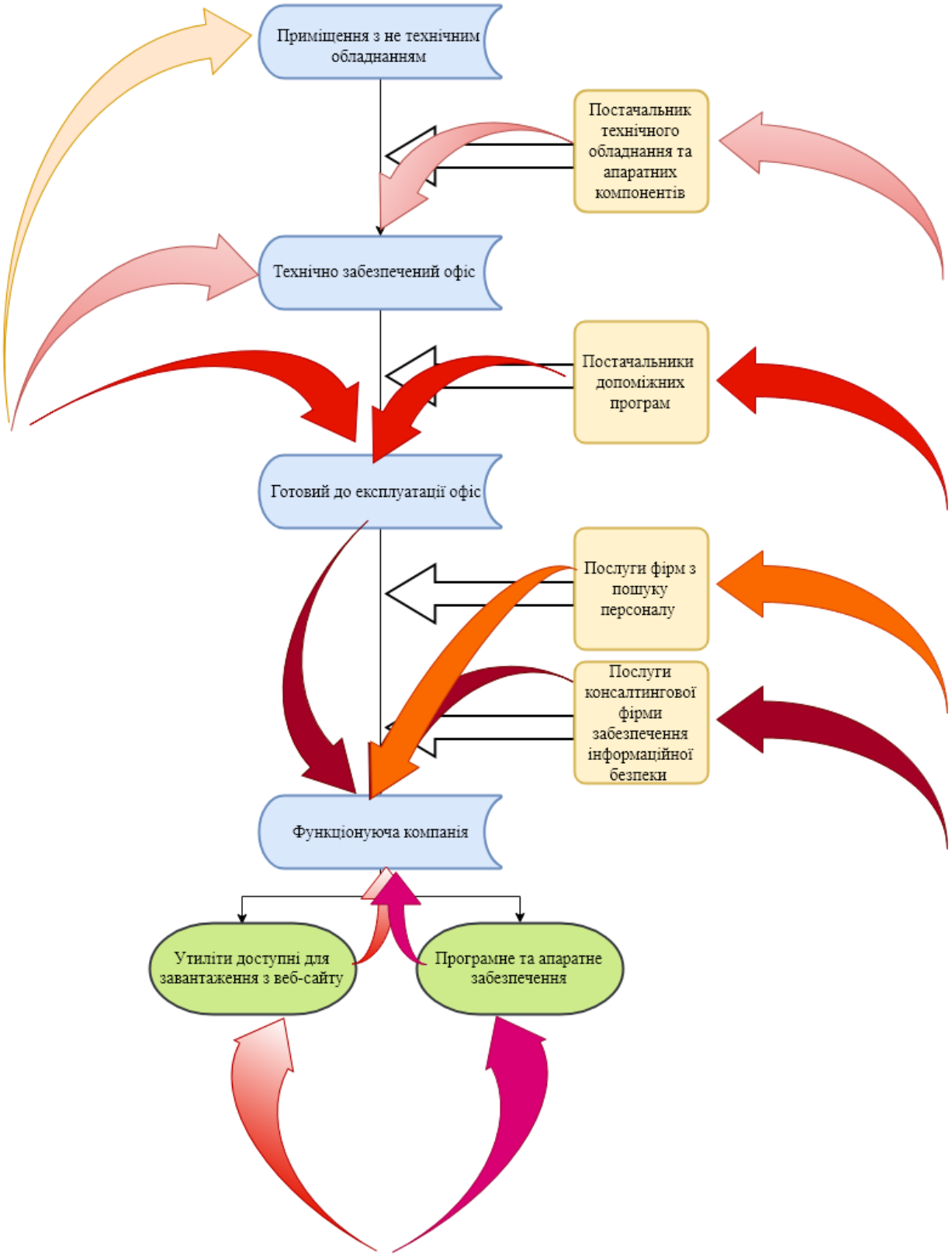

Рисунок 2.3 – Можливі вразливі місця в процесі розвитку і становлення компанії

2.2 Створення методів захисту від атаки на ланцюг постачання на кожному етапі

Перший вид – атака починається з нападу на приміщення з не технічним обладнанням. На цьому кроці в новій компанії навряд чи можлива атака, бо про неї ніхто не знає і вона не становить явної загрози, але якщо компанія відома та користується попитом, відкриває філіал, то цей етап становить серйозну загрозу. Загрози:

1. У момент облаштування офісу може бути встановлений підслуховуючий пристрій, який може встановити вантажник меблів або певна особа, яка може пройти в приміщення.
2. Встановлення шпіонської wi-fi мікрокамери.
3. Фотографування облаштованого приміщення і викладання в соціальні мережі.
4. Завалене мотлохом приміщення, тоді вірогідність успішного здійснення першого та другого пунктів зростає.
5. Наявність в телефоні співробітника підслуховуючого пристрою.

Якщо дані загрози буде успішно втілено в життя, то отримаємо такі наслідки:

1. Втрата інформації про розташування приміщення, де ймовірно є секретна інформація, про майбутні наміри та інші важливі дані, що надає можливість зловмисникам створення ефективної стратегії здійснення атаки.
2. При процесі облаштування приміщення з’являються не потрібні речі, через які складно помітити встановлену камеру або підслуховуючий пристрій, коли в дизайні офісу панує мінімалізм, помітно будь-яку дрібницю і контролювати появу нових речей не складно.

Одна загроза може бути початком втілення іншої загрози, то дані рішення слід втілювати комплексно до цього етапу. Вони мають високу ціну, але в майбутньому ціна втраченої інформації може бути набагато більшою.

Рішення:

1. Скористатися послугами спеціаліста з пошуку підслуховуючих пристроїв в приміщенні та телефонах, жучків, камер і т.д..
2. На вході в офіс встановити металошукачі для людей, та речей, систему реєстрації та контролю співробітників та відвідувачів.
3. Обмежений вхід для не співробітників компанії.
4. Якщо особа має статус гостя – втілюються спеціальні дії:
    - Заклеїти камери смартфона одноразовими наліпками
    - Перевірити речі на наявність пристроїв зчитування інформації
    - Розповісти про правила поводження у офісі та про покарання, при недодержанні правил.
5. Контроль та перевірка появи нових речей в офісі.

Правила для співробітників будуть розглянуть в іншому пункті, але їх додержання обов'язкове і на цьому етапі.

Другий етап – постачальник технічного обладнання. З появою техніки починається плідна робота. Усі дані будуть зберігатися у комп'ютері, а варіантів вкрасти їх безліч. Але можна виокремити дві категорії:

- Використовуючи програми, для вторгнення в систему, викрадення інформації і виведення з ладу системи або непомітне зникнення.
- Використовуючи апаратні засоби для зчитування клавіатурного почерку, паролів і тому подібне.

Антивіруси постійно шукають нові шляхи виявлення вірусів та атак. Якщо зловмисник вирішить примітивним чином поширити вірус, то зіштовхнеться з великою ймовірністю закінчити атаку невдачею, не встигнувши її розпочати. Тому для успішної реалізації атаки хакер використовує спочатку другу категорію, знаходить і відкриває доступ до потрібної папки, наприклад з прописаною стратегією розвитку компанії на найближчі півроку, впроваджує експлойт, з допомогою нього захвачує доступ та краде дані, або стелс-віруса,

який це все робить непомітно. Отже, розглянемо стійкість системи захисту компанії до другої категорії.

Загрози:

1. Чіп в материнській платі, для отримання віддаленого доступу до пам’яті комп’ютера та шпіонажу.
2. GSM жучок у клавіатурі прослуховує звуки в радіусі 10 метрів та заряджається від комп'ютерного роз'єму USB, що використовується клавіатурою.
3. Безпровідний апаратний keylogger, для зчитування усіх натисків на клавіші клавіатури.
4. Апаратна закладка на USB, що надає бездротовий міст до цільової мережі, а також завантаження експлойтів у цільову систему.
5. Апаратна закладка, що дозволяє перехопити сигнал від VGA монітора.

При успішній роботі і впровадження даних апаратних засобів може втілитися у життя такий сценарій:

1. Зчитування паролів і отримання доступу до закритих директорій.
2. Виявлення комп’ютерів, серверів і т.д. , що мають особливо важливі дані і встановлення у них засобів зчитування.
3. Інформація про політику безпеки у компанії, знаходження у ній вразливих сегментів.
4. Вивчення поведінки співробітників та знаходження часу, коли аномальну поведінку комп’ютера вони не помітять.
5. Зчитування клавіатурного почерку.

Отже, втрата даних призведе до більш глобальних процесів розвитку атаки.

Для знайдення апаратних закладок можна використовувати такі **рішення**:

1. Так як закладка може бути вбудована ще в компанії постачальника і отримана техніка в компанію потрапить вже інфікована, то після отримання і перед встановлення техніки в офіс потрібно залучити фахівця, що напередодні вивчить склад даної техніки і перевірить можливі місця

розміщення апаратних закладок на їх наявність та перевірить чесність та надійність постачальника.

2. Створення паспорту постачальника та перевірка його надійності. Детальніше про це в іншому пункті.
3. Встановлення камер спостереження і відділ охорони, яка буде моніторити і відслідковувати підозрілу поведінку співробітника.
4. Контроль робочого місця, відсутність непотрібних речей на робочому столі.
5. Спеціальне приміщення для серверної, паперових носіїв з секретною інформацією, комп'ютерів керівників відділів.

Звісно, людський фактор одна з найбільших загроз, але для зниження її появи є ряд правил, які описано буде далі.

Третій вид – постачальники допоміжних програм. Як мінімум потрібна корпоративна пошта, її застосунок для зручності завантажують на ПК, середовище для написання коду або інші інструменти для роботи, антивірус і програма для очищення та оптимізації операційних систем. Розглянемо можливі загрози.

Загрози:

1. Усі види шкідливого spyware.
2. Програмний keylogger.
3. Оновлення для застосунків, яке вже інфіковане.
4. Спам, фішинг і інші можливі атаки на корпоративну пошту.

Можливі наслідки:

1. Отримання доступу до корпоративної пошти, викрадення інформації та віддання наказів, використовуючи маску керуючого.
2. Перехід по невідомим посиланням може призвести до завантаження вірусу.
3. Отримання даних співробітників та клієнтів, викрадення їх грошей та шантажування для досягнення конкретних цілей.
4. Викрадення інтелектуальної власності компанії.

5. Нищівний удар по репутації компанії.

Рішення:

1. Оцінка ризиків втрати певного виду даних.
2. Розподілення комп’ютерів за наявністю певного виду даних.
3. Розробка для кожного комп’ютера певного сценарію дій антивірусу та застосування конкретних функцій, вибір яких визначається спираючись на тип інформації, яка зберігається в комп’ютері; програми, які встановлені; можливі шляхи зараження комп’ютеру і передбачувані шкідливі програми.
4. Зберігання стратегій, нових розробок, рішень та інтелектуальної власності на комп’ютері, який не має доступу в інтернет і не пов'язаний з іншими пристроями.
5. Пояснення правил користування поштою, заборона переходу по невідомим посиланням та використання в особистих цілях.
6. Налаштування політики безпеки: обмеження прав доступу для співробітників. Вони мають доступ лише для тих ресурсів, які їм потрібні для роботи.
7. Постійний аналіз аномалій в мережевому трафіку.

Отже, це один з найнебезпечніших етапів, який відкриває доступ майже до усієї інформації, втрата якої може знищити компанію.

Четвертий крок – викрадення даних використовуючи фірми з пошуку персоналу. Зазвичай вони мають великі бази даних, в яких міститься усе досьє про співробітника, включаючи дані кредитних карток, інформацію про сімейний стан, наявність дітей, попередній заробіток, судимість і т.д.. Так як найпоширеніша причина вдалої атаки, або викрадення інформації – помилка людини або гра на людських слабкостях (методи соціальної інженерії), тому укомплектування штабу співробітників важливий етап.

Загрози:

1. Отримання доступу до бази даних співробітників.
2. Отримання доступу до бази даних клієнтів.

Рішення:

1. При появі кандидата на посаду, проводиться збір інформації про нього, і визначається рівень його небезпеки, тобто при яких умовах він може зашкодити компанії, який ризик для неї він створює.
2. Обов'язковими пунктами має бути: судимість (була чи ні), сімейний стан(шантаж на основі сім'ї), погані залежності (ігроман, наркоман), місця роботи та причини звільнення, посада, медична карта.
3. Створення спеціальних правил для співробітників та підпис контракту про їх дотримання та не розголошення інформації, з вказаним матеріальним стягненням у разі порушення або не дотримання його.
4. Проходження щорічних курсів підвищення рівня обізнаності захисту інформації у компаніях, навчання найважливішим правилам з забезпечення захисту інформації для співробітників.
5. Створення заходів для підтримання дружелюбної та легкої атмосфери, щоб не виникало ненависті до роботи.
6. Періодичне нагадування нижченаведених правил компанії.
7. Створення сприятливих умов роботи для усіх співробітників.

Правила: (деякий витяг)

1. Чистота робочих поверхонь.
2. Не створювати фото в офісі і не викладати їх у соціальні мережі.
3. Не розголошувати інформацію про місце роботи, план офісу, секретну інформацію і таке інше.
4. Звертати увагу на появу незвичайних речей в офісі.
5. Нікому не передавати свій пропуск.
6. Не встановлювати прослуховуючих засобів.
7. Виконувати настанови спеціалістів з відділу захисту інформації.
8. Не передавати нікому пароль.

Іноді, здійснення атаки залежить від дрібниці, і дякуючи спостережливості співробітника, атака може закінчитись так і не розпочавшись. Тому людський фактор може зіграти і на користь компанії.

П’ятий крок – атака використовує постачальника, який надає послуги з забезпечення інформаційної безпеки та аудиту. Дана фірма відповідає за дотримання всіх норм встановлених для безпечного функціонування компанії на кожному етапі її розвитку. Тобто будь-яка загроза, яка виникає, за знищення, знешкодження та обробку інцидентів відповідальною є дана фірма, в кращому випадку відділ. Якщо в результаті атаки, усі засоби для захисту інформації виведені з ладу, компанія втрачає майже всю інформацію, доступ до якої можна отримати шляхом віддаленого доступу.

Загрози:

1. Отримання вірусу захованого в антивірусі.
2. Використання усіх функцій антивірусу призведе до довгого процесу роботи і не якісного захисту для конкретних цілей.

Рішення:

1. Використання антивірусів з оновленою базою сигнатур, новими методами та підходами до виявлення нових шкідливих програм.
2. Використання програм, які слідкують за поведінкою в мережі, в системі, виявляють аномальну поведінку, та повідомляють про неї.
3. Контроль даних постачальників.
4. Політика паролів:
    - Для адміністраторів довжина паролів 16, для користувачів 8.
    - Обов’язкове використання спец символів, кількість неповторюваних паролів;
    - максимальний термін дії пароля 90 днів;
    - паролі повинні задовольняти вимогам щодо складності.
5. Контроль місця, де фізично зберігаються дані компанії.

6. Точний список, кількість і імена системних адміністраторів у постачальників, які керують системами, які містять дані компанії.
7. Шифрування секретних даних та даних при передачі.
8. Аудит, виправлень програмного забезпечення від відповідних постачальників програмного забезпечення, що встановлені на комп'ютерах ваших постачальників своєчасно.
9. Перевірка нових програм, оновлень, версій антивірусів на окремій віртуальній машині, перед тим, як вбудовувати у систему усієї компанії.
10. Перевірка, політики постачальника щодо доступу до систем як для активних, так і для звільнених співробітників (включаючи зміну / скасування імені користувача і пароля) часто розглядаються / переглядаються всіма співробітниками.
11. Перевірка політики постачальника щодо портативних пристроїв і безпеки ноутбука.
12. Перевірка постачальника процедур безпеки бездротової мережі і можливості моніторингу.
13. Резервне копіювання всіх важливих даних здійснюється постійно і часто.
14. Аудит, постачальників на підтримання всіх брандмауерів та антивірусного програмного забезпечення до останніх версій.
15. Регулярна перевірка всіх прав доступу / доступу до «критично важливих» файлів.
16. Обов’язкова наявність документованого і протестованого плану аварійного відновлення та оповіщення про ризики.
17. Перед заключенням контракту з постачальником створити його паспорт постачальника, компонентами якого мають бути:
    - Назва підприємства
    - Початок роботи з постачальником і закінчення (має бути укладена угода)
    - Відділи, які співпрацюють з постачальником

- Інформація компанії, якою оперує і має в доступі постачальник
- Постачальники, з якими співпрацює даний постачальник
- Список компаній, з якими співпрацював/співпрацює постачальник
- Методи захисту інформації, які використовує постачальник
- Згоду на аудит постачальника, що проведуть спеціалісти компанії, яка використовує послуги цього постачальника.

18. Оцінювання ризиків для компанії при реалізації загрози та розробка для кожного комп'ютера, за величиною ризику та можливих атак, спеціального сценарію захисту інформації методами антивірусу.
19. Коректне знищення та видалення інформації.
20. Обробка інцидентів.
21. Використання захищених віртуальних приватних мереж (Virtual Private Network ─ VPN) дозволить вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам.
22. Постійні рейди аудиту в компанії постачальників.
23. Постійно оновлювати паролі.
24. Постійний розвиток і підвищення класифікації відділу (компанії) захисту інформації.

Розглянемо загрози на веб-сервер зі сторони атаки на ланцюг поставок. Є основних два варіанти:

- На веб-сайт завантажують оновлення, новий застосунок або іншу програму, що вже інфікована вірусом, яку користувачі можуть завантажити, після запуску програма блокує комп'ютер, і користувач отримує повідомлення з планом дій, щоб повернути інформацію, від зловмисника-вимагача.
- Зловмисник перехоплює пароль адміністратора веб-сайту, створює маску сайту (отримує дані клієнтів, які заповнюють форму) або проводить DoS або DDos (або іншу атаку) і використовують вразливості ПЗ, щоб вивести з ладу, або надсилання флуду, а сервер витрачає всі

ресурси машини на обробку запитів, що атакують, а користувачам доводиться чекати.

Якщо в компанії на перших етапах було сховане апаратне або програмне шпіонське ПЗ, то на цьому етапі, зловмисник вже має інформацію, коли фахівець може бути відсутнім на робочому місці і знати найвдаліший час для проведення атаки DoS або DDos (або іншої) і завантаження інфікованого ПЗ на сайт.

Коли вже створено нове апаратне і програмне забезпечення, залишається створити багато копій та надіслати у магазини збуту. Але на цьому етапі теж можлива загроза.

Загроза:

1. Неякісне виготовлення продукції, що тягне за собою втрату репутації компанії.

Рішення:

1. Аудит виробництва.
2. Ретельна перевірка перед випуском продукції.

2.3 Оцінка небезпеки загрози

Для створення формули розрахунку небезпеки загрози використаємо 5 аспектів оцінки:

1. Цінність інформації, яку втратимо в результаті успішної атаки.
2. Скільки дій для захисту інформації існує, для виявлення та зупинення атаки.
3. Складність шляху атаки для отримання потрібної інформації.
4. Ризик для компанії, якщо співробітник буде підставним обличчям.
5. Кількість співробітників, які мають доступ до комп’ютера, де може бути реалізована загроза.

Якщо є декілька можливих варіантів в 1 пункті, то вибираємо показник цінності найважливішої інформації. Оцінювання інформації наведено в таблиці 2.1.

Таблиця 2.1 – Цінність інформації, яку втратимо в результаті успішної атаки

Інформація	Показник цінності
Не зашифровані персональні дані	5
Зашифровані персональні дані	4
Не зашифровані дані, що є інтелектуальною власністю компанії	5
Зашифровані дані, що є інтелектуальною власністю компанії	4
Паролі входу в комп’ютер	3
Паролі входу в базу даних, папку з секретною інформацією і т.д.	5
Паролі входу в корпоративну пошту	4
Інформація, потрібна зловмиснику для побудови стратегії атаки	1
Інформація про постачальників	2

Скільки дій для захисту інформації існує, для виявлення та зупинення атаки?!

Чим більша кількість дій для виявлення та зупинення атаки, тим менша ймовірність її реалізації, тому доречно знайти найбільшу кількість дій, наприклад 20 і взяти по модулю (найбільша кількість дій + 1), тобто 21. Таким чином отримаємо потрібний нам показник, який потрібно використати у в формулі.

Відносну складність шляху атаки для отримання потрібної інформації наведено в таблиці 2.2. Чим складніше дістатися до цілі, тим менша ймовірність реалізації загрози. Тобто якщо вірус потрапляє у систему, йому потрібно здійснити певні дії (підібрати пароль, знайти потрібну директорію і т.п.), чим

більша їх кількість – тим більша ймовірність того, що помітять аномальну поведінку на певному комп’ютері і встигнуть зупинити атаку.

Таблиця 2.2 – Складність шляху атаки для отримання інформації.

Шлях атаки	**Відносна складність**
Перейти в даному комп’ютері в певну директорію	4
Перейти в даному комп’ютері в певну директорію з паролем	3
Перейти з даного комп’ютера на інший	4
Перейти в базу даних	2
Потрапити в комп’ютер, сейф, т.д.	5
Потрапити на сервер	2
Потрапити у комп’ютер директора	1
Потрапити у комп’ютер керівника відділу захисту інформації	1

Людина – не ідеальна машина, тому не варто не до оцінювати ризики для компанії створені людиною. До 80% всіх комп'ютерних злочинів пов'язано з спеціальними або ненавмисними внутрішніми порушеннями з боку працюючих або звільнених співробітників. Для оцінювання ризику співробітника, про нього потрібно зіставити таблицю 2.3 та оцінити кожен пункт.

Таблиця 2.3 – Тест, що складається для кожного співробітника.

Факти	**Так(1) / Ні(0)**
Наявність сім’ї	1
Працював в компанії конкурента	1
Невідомі причини звільнення з попереднього місця роботи	1
Наявність судимості	0
Наявність залежностей (ігроман, наркоман)	0
Наявність психічних захворювань	0
Наявність кредитів, боргів	0
Наявність високої посади	1

Для кожного співробітника створюється така таблиця і заповнюється, за кожну відповідь «так» до 1 додаємо 1 бал, (1 початкове значення), і так до кінця заповненої таблиці. Потім кількість отриманих балів ділимо на кількість фактів

плюс 1, тобто 9, наприклад 4 бали в таблиці, отже (4+1)/9 ≈ 0.55 – ймовірність зради компанії співробітником, який заповнив таблицю.

Використовуючи дані про кількість співробітників можна вивести формулу. Нехай k – це кількість співробітників, які мають доступ до комп'ютера, де може бути реалізована загроза.

Якщо k = 1, то маємо скорочену формулу:

$$R = \frac{\sum_{i=1}^{3} A + (P(h) * 100\%)}{5} \qquad (2.1)$$

де, A_1 – цінність інформації;

q – кількість дій;

max – максимальна кількість дій для захисту інформації існує, для виявлення та зупинення атаки;

A_2 – показник кількості дій, потрібних для виявлення та зупинення атаки;

$A_2 = q \bmod(max + 1)$

A_3 – складність шляху атаки;

h – подія, коли співробітник активував загрозу;

P(h) – ймовірність зради компанії співробітником;

Якщо k > 1, то :

h1 – подія, коли співробітник 1 активував загрозу;

h2 – подія, коли співробітник 2 активував загрозу;

h3 – подія, коли співробітник 3 активував загрозу;

І т.д., в залежності від кількості співробітників, які мали доступ до комп'ютера, де може бути реалізована загроза.

P(h1) – ймовірність події h1, аналогічно P(h2), P(h3) і т.д..

P($\overline{h1}$) = 1- P(h1) – ймовірність не здійснення події h1, аналогічно P($\overline{h2}$), P($\overline{h3}$) і т.д..

Тоді потрібно знайти ймовірність події h, коли хтось один атакує.

$$h = \overline{h1} \cdot \overline{h2} \cdot h3 + \overline{h1} \cdot h2 \cdot \overline{h3} + h1 \cdot \overline{h2} \cdot \overline{h3}$$

Використовуючи теореми додавання і множення маємо ймовірність виконання події h, як сума добутків ймовірності настання однієї події і не настання інших, для 3 співробітників формула виглядає таким чином:

$$P(h) = P(\overline{h1}) \cdot P(\overline{h2}) \cdot P(h3) + P(\overline{h1}) \cdot P(h2) \cdot P(\overline{h3}) + P(h1) \cdot P(\overline{h2}) \cdot P(\overline{h3})$$

Тоді підставляємо в (2.1), якщо доступ до комп'ютера мало більше 1 співробітника.

Наприклад, якщо вхідні дані:

Порушник отримав віддалений доступ до комп'ютера(доступ має 3 співробітника з один – сім'янин, другий працював у компанії конкурента, а третій – сім'янин, що має високу посаду), де зберігаються зашифровані дані, що є інтелектуальною власністю компанії, тоді маємо :

$A_1 = 4$,

q = 7,

max = 20,

$A_3 = 3$,

P(h1) = (1+1)/9 = 0.22 P($\overline{h1}$) = 1 – 0.22 = 0.88

P(h2) = (1+1)/9 = 0.22 P($\overline{h2}$) = 1 – 0.22 = 0.88

P(h3) = (1+2)/9 = 0.33 P($\overline{h3}$) = 1 – 0.33 = 0

$$R = \frac{A_1 + \mathrm{q}\bmod(\max+1) + A_3 + (P(\overline{h1}) \cdot P(\overline{h2}) \cdot P(h3) + P(\overline{h1}) \cdot P(h2) \cdot P(\overline{h3}) + P(h1) \cdot P(\overline{h2}) \cdot P(\overline{h3})) * 100\%}{5}$$

$$\mathrm{R} = \frac{(4 + 7\bmod 21 + 3) + (0.88 \cdot 0.88 \cdot 0.33 + 0.88 \cdot 0.22 \cdot 0.77 + 0.22 \cdot 0.88 \cdot 0.77) * 100\%}{5} =$$

$$\frac{(21 + (0.25 + 0.15 + 0.15) * 100\%)}{5} = \frac{76}{5} = \mathbf{15.2}$$

Для визначення шкали успішної реалізації потрібно оцінити загрозу з мінімальними та з максимальними даними.

Модель для захисту інформації на підприємстві від атаки на ланцюг постачання

Модель розроблено на основі положень вже існуючої політики безпеки. Тобто, рішення, запропоновані вище, спрямовані на адаптування політики безпеки до

захисту від атаки на ланцюг постачання, але так як атака використовує вразливі місця, то дані рішення покращують ефективність будь-якої політики безпеки.

2.4 Особливості та рекомендації щодо впровадження моделі захисту

Модель має певні особливості. Чотири основні з них – це створення паспорту постачальника, запровадження пошуку досьє на кожного співробітника компанії, атмосфера в компанії та налагодження сценарію дій антивірусу. Для цього є об’єктивні причини. Проаналізувавши усі успішно реалізовані атаки на ланцюг постачання, можна переконатися, що повна довіра до постачальника – це невиправданий ризик. Через його недбалість і халатне відношення до безпеки своєї компанії зростає ймовірність втрати репутації, партнерів, коштів для нього та компаній, що співпрацюють з ним. Тому при поширенні такого типу атаки, загрозу можна зупинити на моменті реалізації її у постачальника. І якщо вже атака пройшла, то компанія постачальника повинна отримати покарання за це і не мати змогу зняти з себе відповідальність.

Друга особливість – перевірка кожного майбутнього співробітника. До 80% всіх комп'ютерних злочинів пов'язано з спеціальними або ненавмисними внутрішніми порушеннями з боку працюючих або звільнених співробітників. У кожного може бути свій мотив, але є певні фактори в біографії кожної людини, які не можна не враховувати. Якщо людина має діагноз, результатом якого може бути втрата контролю над собою або бажання помсти за звільнення чи з я певних особистих причин.

Третя – це звернення уваги на моральний стан людини. Якщо робота проходить в жорсткому контролі та під тиском, складно відчувати себе вільним та не відчувати відрази до роботи. У всьому світі популярне явище тимбілдинг, або командотворення (англ. Team building), для створення командного духу в компанії та зняття стресу. Це забезпечує нормальний психологічний стан кожного співробітника, збільшення ефективності та запобігання ненависті до

компанії. Постійна практика введення заохочень, відпусток, врахування годин роботи в неробочий час.

Четверта – це налагодження сценарію дій антивірусу. Так як використовування усіх функцій для захисту комп'ютера з певним видом інформації може створити додаткові вразливості для системи, то слід розробити для кожного типу свій сценарій, що перевіряє та захищає від типу загроз притаманному даній системі.

Для застосування моделі для компанії потрібно застосувати ряд кроків:

1. Перевірити ділянки на наявність загроз і створити список знайдених.
2. Для кожної загрози у списку створити оцінку успішної реалізації загрози, використовуючи формулу (2.1).
3. Застосувати усі рішення, запропоновані в попередньому розділі.
4. Оцінити загрози зі списку при нових умовах.
5. Їх ймовірність зменшиться, але не зникне, тому потрібно сортувати загрози від найвищої ймовірності до найнижчої.
6. Ретельно відслідковувати загрози, що представляють найбільшу загрозу.

Висновки до розділу 2

Було розглянуто схему атаки на ланцюг постачання та виявлено вразливості на кожному етапі. Для ефективного проектування моделі захисту, проходило оцінювання кожного етапу атаки, виявлення основних загроз та створення певного набору рішень для того, щоб вчасно виявити, зупинити та знищити атаку на початку. З аналізу найбільших атак у 2 розділі було виявлено 5 основних характеристик загрози в розрізі атаки на ланцюг постачання. І за їх оцінюванням виведено формулу для оцінки небезпеки загрози з точки зору даної атаки. За допомогою формули можна оцінити усі загрози і стратегічно правильно застосувати запропоновані методи захисту.

3 ОЦІНКА ЕФЕКТИВНОСТІ СТВОРЕНОЇ МОДЕЛІ

Розглянемо вже створену політику безпеки, проаналізуємо скільки запропонованих рішень можна втілити для її покращення та оцінимо їх ефективність.

Політика інформаційної безпеки розроблена відповідно до:

– закону України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 № 80/94-ВР;

– постанови Кабінету Міністрів України від 27.11.98 № 1893 “Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію”;

– постанови Кабінету Міністрів України від 29.03.2006 № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах”;

– державних стандартів України в галузі технічного захисту інформації

3.1 Розгляд існуючої політики безпеки

Розглянемо вже існуючу політику безпеки у таблиці 3.1.

Таблиця 3.1 – Політика безпеки.

№	Положення політики інформаційної безпеки
1.	Вхідні двері обладнані замками, що гарантують надійне закриття приміщень в неробочий час.
2.	Приміщення обладнані охоронною та пожежною сигналізацією.
3.	Умови розміщення обладнання відповідають вимогам техніки безпеки, санітарним нормам і вимогам пожежної безпеки.

Продовження таблиці 3.1

№	Положення політики інформаційної безпеки
4.	Запасні ключі від серверної зберігаються в опечатаному пеналі в сейфі у начальника ВРО.
5.	Підключення корпоративної мережі державного підприємства до Інтернету здійснюється через міжмережевий екран.
6.	Весь вхідний і вихідний трафік проходить через фільтри брандмауера (міжмережевий екран).
7.	Брандмауер адмініструється локально або віддалено з фіксованої адреси адміністратора.
8.	У налаштуванні міжмережевого доступу закриті всі сервіси та протоколи, що не використовуються. Програмний захист міжмережевого екрану постійно оновлюється. Для міжмережевого екрану допускається лише один користувач – адміністратор, решта користувачів видалені або заблоковані.
9.	Доступ користувачів до мережі Інтернет здійснюється тільки через міжмережевий екран.
10.	Брандмауер веде детальні системні журнали всіх сеансів. Доступ до журналів має обмежена кількість співробітників підприємства.
11.	На брандмауері ведуться "Стоп аркуші" ресурсів Інтернет сумнівного змісту. Брандмауер дозволяє завантаження тільки тих програм, які дозволені.
12.	Операційні системи та програмне забезпечення серверів повинні містити всі виправлення, рекомендовані виробником.
13.	Сервери підприємства, що працюють під UNIX подібними операційними системами, не запускаються з правами суперкористувача.
14.	Доступ до Інтернету здійснюється тільки через брандмауер підприємства.

Продовження таблиці 3.1

№	Положення політики інформаційної безпеки
15.	Кожен завантажений файл повинен перевіряється на віруси і троянські програми.
16.	Користувачам без особливого дозволу забороняється встановлювати і використовувати зовнішні поштові сервери.
17.	Електронні документи, що містять службову інформацію, не повинні відправлятися за допомогою електронної пошти по відкритих каналах в не зашифрованому вигляді.
18.	Користувачі використовують тільки дозволені адміністратором мережі поштові програми.
19.	Ніхто з відвідувачів підприємства або тимчасових співробітників не має права використовувати електронну пошту підприємства.
20.	Поштові сервери налаштовані так, щоб відкидати листи, адресовані не домену підприємства.
21.	Контроль виконання заходів з інформаційної безпеки при роботі в мережі Інтернет і використанні електронної пошти покладається на адміністратора комп'ютерної мережі.
22.	На всіх робочих станціях встановлений антивірусний контроль з автоматичним періодичним оновленням антивірусних баз і автоматичним запуском антивірусного монітора.
23.	Використання на робочих станціях дискових ресурсів із загальним доступом допускається тільки у виняткових випадках.
24.	Використання на робочих станціях накопичувачів зі з'ємними машинними носіями інформації і портів USB допускається у виняткових випадках.
25.	Використовувати персональний комп'ютер і ресурси комп'ютерної мережі підприємства тільки для виконання своїх службових обов'язків.

Продовження таблиці 3.1

№	Положення політики інформаційної безпеки
26.	Зберігати робочі матеріали і документи в електронному вигляді на спеціально виділеному каталозі файлового сервера.
27.	Блокувати робочу станцію за необхідності покинути робоче місце на нетривалий час.
28.	Вимикати робочу станцію, покидаючи робоче місце на тривалий час.
29.	Забороняється входити в комп'ютерну мережу підприємства, використовуючи чужі реквізити доступу.
30.	Забороняється залишати без нагляду підключене і не заблоковане робоче місце.
31.	Забороняється відключати антивірусне програмне забезпечення встановлене на їх робочих станціях, і змінювати його налаштування.
32.	Забороняється завантажувати з мережі Інтернет програмне забезпечення.
33.	Забороняється дозволяти іншим особам роботу на комп'ютері зі своїми правами доступу.
34.	Забороняється самостійно змінювати апаратну або програмну конфігурацію робочих станцій
35.	Забороняється самостійно встановлювати на робочу станцію програмне забезпечення.
36.	Інформація про паролі користувачів є службовою інформацією, яка призначена для ідентифікації та допуску кожного конкретного користувача до виділених йому інформаційних ресурсів.
37.	Паролі адміністраторів і паролі серверів зберігаються в опечатаних конвертах у сейфі. Кожен пароль зберігається в окремому конверті.
38.	Операційні системи серверів та робочих станцій блокують вхід в мережу після 3-х кратної помилки в наборі пароля.

Продовження таблиці 3.1

№	Положення політики інформаційної безпеки
39.	В разі звільнення працівника з підприємства, системний адміністратор, на підставі обхідного аркуша, робить видалення імені користувача з інформаційної системі підприємства.
40.	У разі відпустки співробітника підприємства системний адміністратор, на підставі заявки керівника структурного підрозділу, блокує ім'я користувача в інформаційній системі підприємства.
41.	Налаштування активного мережевого обладнання підприємства (маршрутизатори, комутатори) не дає можливості несанкціонованої переконфігурації, в зв'язку з чим, кожний активний мережевий пристрій захищений унікальним паролем адміністратора комп'ютерної мережі.
42.	Адміністраторам різних інформаційних систем забороняється використання адміністративного пароля у повсякденній діяльності, не пов'язаної з адміністративними функціями. Для цієї мети адміністраторам повинен виділятися пароль з правами користувача.
43.	Операційні системи робочих станцій налаштовані таким чином, щоб блокувати паузи неактивності (зберігач екрану) з функцією парольного захисту. Час включення захисту не більше 15 хвилин.
44.	Операційні системи серверів налаштовані таким чином, щоб виключити можливість ознайомлення з парольною інформацією будь-якого з користувачів, окрім адміністратора та керівника служби безпеки інформації.
45.	Операційні системи робочих станцій, включених в комп'ютерну мережу підприємства, мають параметри, що дозволяють виключити можливість перегляду введеної парольної інформації.
46.	Період дії паролів становить 90 діб, після чого вони підлягають заміні на нові, які раніше не застосовувалися.

Кінець таблиці 3.1

47.	Якщо немає можливості зробити копіювання, проводиться роздруківка конфігураційних файлів. Резервні копії зберігаються до закінчення їх актуальності.
48.	Резервні копії створюються після першого налаштування або внесення змін до налаштування операційних систем серверів, програмного забезпечення серверів та мережевого обладнання на з'ємних машинних носіях;

3.2 Формування набору рішень для даної політики безпеки

Отже, розглянемо, які рішення можна втілити для покращення ефективності роботи політики безпеки:

1. Скористатися послугами спеціаліста з пошуку підслуховуючих пристроїв в приміщенні та телефонах, жучків, камер і т.д..
2. На вході в офіс встановити металошукачі для людей, та речей, систему реєстрації та контролю співробітників та відвідувачів.
3. Обмежений вхід для не співробітників компанії.

Якщо особа має статус гостя – втілюються спеціальні дії:

4. Заклеїти камери смартфона одноразовими наліпками
5. Перевірити речі на наявність пристроїв зчитування інформації
6. Розповісти про правила поводження у офісі та про покарання, при недодержанні правил.
7. Контроль та перевірка появи нових речей в офісі.
8. Перевірка техніки перед встановленням в офіс.
9. Створення паспорту постачальника.
10. Встановлення камер спостереження і відділ охорони, для моніторингу дій співробітника.

11. Контроль робочого місця, відсутність непотрібних речей на робочому столі.
12. Розподілення комп’ютерів за наявністю певного виду даних та розробка для кожного комп’ютера певного сценарію дій антивірусу.
13. Зберігання інтелектуальної власності компанії на комп’ютері, який не має доступу в інтернет і не пов'язаний з іншими пристроями. Налаштування політики безпеки: обмеження прав доступу для співробітників.
14. Пошук досьє та оцінка ризику для компанії кожного співробітника.
15. Проходження щорічних курсів підвищення рівня обізнаності захисту інформації у компаніях, навчання найважливішим правилам з забезпечення захисту інформації для співробітників.
16. Створення заходів для підтримання дружелюбної та легкої атмосфери, щоб не виникало ненависті до роботи. Створення сприятливих умов роботи для усіх співробітників
17. Періодичне нагадування нижченаведених правил компанії.

    Правила: (деякий витяг)
18. Чистота робочих поверхонь.
19. Не створювати фото в офісі.
20. Звертати увагу на появу незвичайних речей в офісі і не встановлювати прослуховуючих засобів.
21. Використання програм, які слідкують за поведінкою в мережі, в системі, виявляють аномальну поведінку, та повідомляють про неї.
22. Контроль даних постачальників.
23. Точний список, кількість і імена системних адміністраторів у постачальників, які керують системами, які містять дані компанії.
24. Аудит, виправлень програмного забезпечення від відповідних постачальників програмного забезпечення, що встановлені на комп'ютерах ваших постачальників своєчасно.
25. Перевірка нових програм, оновлень, версій антивірусів на окремій віртуальній машині, перед тим, як вбудовувати у систему усієї компанії.

26. Перевірка, політики постачальника щодо доступу до систем як для активних, так і для звільнених співробітників (включаючи зміну / скасування імені користувача і пароля) часто розглядаються / переглядаються всіма співробітниками.
27. Перевірка політики постачальника щодо портативних пристроїв і безпеки ноутбука.
28. Перевірка постачальника процедур безпеки бездротової мережі і можливості моніторингу.
29. Аудит, постачальників на підтримання всіх брандмауерів та антивірусного програмного забезпечення до останніх версій.
30. Регулярна перевірка всіх прав доступу / доступу до «критично важливих» файлів.
31. Обов'язкова наявність документованого і протестованого плану аварійного відновлення та оповіщення про ризики.
32. Політика паролів.
33. Оцінювання ризиків для компанії при реалізації загрози та розробка для кожного комп'ютера, за величиною ризику та можливих атак, спеціального сценарію захисту інформації методами антивірусу.
34. Обробка інцидентів.
35. Постійні рейди аудиту в компанії постачальників.
36. Постійний розвиток і підвищення класифікації відділу (компанії) захисту інформації.
37. Ретельна перевірка перед випуском продукції.

3.3 Оцінка ефективності запропонованих методів

Якщо абстрагуватися від факту, що ні одна політика безпеки не є 100% захистом, то нехай політика безпеки, яка розглядається, має ефективність 100%, вона має 48 пунктів, нехай кожен пункт однаково важливий. Кількість

запропонованих рішень складає 37 пунктів, що відрізняються від пунктів, які прописані в політиці безпеки. Отже, $37 \div 48 * 100\% \approx 77.08\%$ – приблизно на стільки відсотків збільшиться ефективність політики безпеки. Оцінивши загрози за формулою (2) можна точніше оцінити ефективність, з підрахунку кількості рішень зменшення ймовірності загрози для кожної. Але цей розрахунок створений як доказ ефективності даної моделі.

Висновки до розділу 3

Використовуючи запропоновану модель створюємо більш ефективний захист проти атаки на ланцюг постачання. Порівнюючи політику безпеки, представлену спочатку, та доповнену запропонованими методами захисту видно, що ефективність значно збільшилась. Тобто, застосування даної системи корисно для захисту від атаки на ланцюг постачання. Так як неможливо створити стовідсоткову захищену робочу систему, але можливо збільшити її надійність, то з точки зору атаки на ланцюг постачання з цю задачу виконано.

ВИСНОВКИ

В даній дипломній роботі було розглянуто такі поняття як ланцюг постачання та атака на нього. Було визначено головні схеми та особливості їх дії, методи захисту від них, загрози, які виникають і як зловмисники їх використовують.

В ході дослідження було визначено:

- Основні вразливості політики безпеки;
- Основні загрози для системи, якими можуть скористатися зловмисники для створення атаки;
- Створення методів захисту від виявлених загроз;
- Оцінка небезпеки загрози;
- Виявлено основні етапи атаки на ланцюг постачання;

Також було розглянуто вже успішно реалізовані атаки, на основі їх аналізу було виявлено основне вразливе місце – постачальники. Вони можуть бути однією з ланок атаки на ланцюг постачання і навіть не знати про це. Тому у відношенні до них було створено ряд дій, таких як створення паспорту постачальника, постійний аудит постачальників постачальника і т.д.. Контролюючи їх можна зупинити атаку на етапі потрапляння її до постачальників, адже не завжди вони використовують усі можливі засоби для захисту інформації.

Так як 80% усіх атак було проведено використовуючи людський фактор, то одним із розглянутих елементів захисту було оцінювання персоналу на наявність ризику викрадення інформації або виведення з ладу системи. У кожної людини може бути мотив зіпсувати роботу компанії, адже є багато причин: шантажування співробітника, підкуп, ненависть до своєї роботи і інші, через що співробітник може піти на зраду. Тому обов’язковим пунктом було оцінювання ризику для компанії, який несе співробітник, адже він має доступ до секретної

інформації або може просто інфікувати потрібний комп’ютер. Налагодження роботи співробітників у команді – це важливий фактор, що недооцінюють.

Також важливим сегментом захисту – є налагодження сценарію дій антивірусу. Найчастіше через антивірус встигає потрапити в систему декілька вірусів, або через надмірність дій і часу перевірки, деякі віруси залишаються не зловленими. Крім звичайних дій оновлення бази сигнатур, потрібно проаналізувати, яка інформація частіше за все обробляється в комп’ютері, який тип загроз найчастіше випливає і створити такий сценарій дій антивірусу, щоб був забезпечений максимальний захист від конкретного типу загроз на конкретному комп’ютері та виконувались функції для загального захисту. Так як використовування усіх функцій для захисту комп’ютера з певним видом інформації може створити додаткові вразливості для системи, то використання сценарію для комп’ютера якому притаманний певний тип загроз забезпечить ефективніший захист.

Було проаналізовано успішно реалізовані атаки та можливі вразливі місця в ланцюгу постачання, створено перелік загроз для кожного етапу ланцюга постачання, визначено найефективніші методи захисту, вдосконалено існуючі методи захисту, створено власну формулу для оцінки небезпеки загрози для компанії та побудовано модель захисту від атаки на ланцюг постачання для інформаційної системи компанії та оцінено її ефективність.

Було наведено поради для запровадження даної моделі захисту та проведено дослідження, що доводить яким чином можна поліпшити існуючу політику безпеки.

Можна зазначити, що результати досліджень доводять ефективність моделі захисту, підвищення рівня захищеності інформації, що знаходиться в інформаційній системі підприємства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Blackmer M. Attacking the Weakest Link in the Supply Chain [Електронний ресурс] / Marc Blackmer // Cisco Blog. – 2017. – Режим доступу до ресурсу: https://blogs.cisco.com/security/attacking-the-weakest-link-in-the-supply-chain?dtid=osscdc000283.
2. Panda Security. Supply chain attack: риски для предприятий от атак на цепочку поставок [Електронний ресурс] / Panda Security // Mediacenter. – 2019. – Режим доступу до ресурсу: https://www.cloudav.ru/mediacenter/news/business-risks-supply-chain-attacks/.
3. ЛУГАНОВСЬКА Є. GDPR в Україні: стратегічний план чи необдумане рішення? [Електронний ресурс] / ЄВГЕНІЯ ЛУГАНОВСЬКА // delo.ua. – 2018. – Режим доступу до ресурсу: https://delo.ua/business/gdpr-v-ukrajini-strategichnij-plan-chi-neobduman-348025/ .
4. Pankov N. Не станьте звеном в атаке через цепочку поставок [Електронний ресурс] / Nikolay Pankov // Kaspersky Lab. – 2018. – Режим доступу до ресурсу: https://www.kaspersky.ru/blog/ccleaner-supply-chain/20045/ .
5. CCleanup: A Vast Number of Machines at Risk [Електронний ресурс] / Edmund Brumaghin, Ross Gibb, Warren Mercer та ін.] // Cisco Talos. – 2017. – Режим доступу до ресурсу: https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html .
6. Нова хвиля кібератак в Україні може поширитись через сайт розробника ПЗ для бухобліку - експерти Детальніше читайте на УНІАН: https://www.unian.ua/science/2095776-nova-hvilya-kiberatak-v-ukrajini-moje-poshiritis-cherez-sayt-rozrobnika-pz-dlya-buhobliku-e [Електронний ресурс] // УНІАН. – 2017. – Режим доступу до ресурсу: https://www.unian.ua/science/2095776-nova-hvilya-kiberatak-v-ukrajini-moje-poshiritis-cherez-sayt-rozrobnika-pz-dlya-buhobliku-eksperti.html.

7. New Ransomware Variant "Nyetya" Compromises Systems Worldwide [Електронний ресурс] // Cisco Talos. – 2017. – Режим доступу до ресурсу: https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.
8. Точно в цель - атака на Target [Електронний ресурс] // Infowatch. – 2014. – Режим доступу до ресурсу: https://www.infowatch.ru/analytics/leaks_monitoring/5196.
9. Target Hackers Broke in Via HVAC Company [Електронний ресурс] // KrebsonSecurity. – 2014. – Режим доступу до ресурсу: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
10. Експерти з кібербезпеки зазначають, що на розшифровування вірусу можуть піти тижні. [Електронний ресурс] // TCH.ua. – 2017. – Режим доступу до ресурсу: https://tsn.ua/ukrayina/u-antivirusnoyi-kompaniyi-rozpovili-hto-mozhe-stoyati-za-hakerskoyu-atakoyu-petya-a-i-chim-ce-zagrozhuye-952457.html.
11. В Україні зафіксували наймасштабнішу кібератаку в історії. // TCH.ua. – 2017. – Режим доступу до ресурсу: https://tsn.ua/ukrayina/robota-ukrayinskih-komp-yuternih-merezh-bude-povnistyu-vidnovlena-za-kilka-dniv-geraschenko-952460.html.
12. Patrick Moorhead. That Time Of Year Again: Cisco Systems Releases Its Annual Cybersecurity Report [Електронний ресурс] / Patrick Moorhead // Forbes. – 2018. – Режим доступу до ресурсу: https://www.forbes.com/sites/patrickmoorhead/2018/03/05/that-time-of-year-again-cisco-systems-releases-its-annual-cybersecurity-report/#3e35b42518ec.
13. Information security breaches survey 2013: technical report [Електронний ресурс] // Gov.uk. – 2013. – Режим доступу до ресурсу: https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report.

14. Managing Cyber Supply Chain Risks [Електронний ресурс] // Advisen Insurance Intelligence. – 2013. – Режим доступу до ресурсу: http://www.advisenltd.com/wp-content/uploads/2013_OBPI_SupplyChainCyberRM_Whitepaper.pdf.
15. Cyber-security risks in the supply chain [Електронний ресурс] // Cert-uk. – 2015. – Режим доступу до ресурсу: https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf.
16. ROB WAUGH. The terrifying rise of cyber crime: Your computer is currently being targeted by criminal gangs looking to harvest your personal details and steal your money [Електронний ресурс] / ROB WAUGH // Mail Online. – 2013. – Режим доступу до ресурсу: https://www.dailymail.co.uk/home/moslive/article-2260221/Cyber-crime-Your-currently-targeted-criminal-gangs-looking-steal-money.html.
17. Supply Chain Risk – the "Cyber Attack" [Електронний ресурс] // ISG – Режим доступу до ресурсу: https://www.isg-one.com/industries/consumer-goods/articles/supply-chain-risk-the-cyber-attack.
18. Elia Florio. Attack inception: Compromised supply chain within a supply chain poses new risks [Електронний ресурс] / Elia Florio, Lior Ben Porat // Microsoft. – 2018. – Режим доступу до ресурсу: https://www.microsoft.com/security/blog/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/.
19. ISO/IEC 28001:2007, Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance.
20. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] // Законодавство України. – 2014. – Режим доступу до ресурсу: https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
21. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію [Електронний ресурс] //

Законодавство України. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1893-98-%D0%BF.

22. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] // Законодавство України. – 2011. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.
23. ISO/IEC 27001:2013, Information technology Security Techniques - Information security management systems — Requirements.